高等学校计算机专业规划教材
国家自然科学基金资助项目教材

信息通信技术供应链安全



吴世忠 江常青 彭勇 陈冬青 陆天波 编著

清华大学出版社

高等学校计算机专业规划教材
国家自然科学基金资助项目教材

信息通信技术供应链安全

吴世忠　江常青　彭　勇
陈冬青　陆天波　编著

清华大学出版社
北　京

内 容 简 介

本书主要介绍与信息通信技术供应链相关的主题，全书共10章，可分为四大部分，首先介绍信息通信技术供应链相关概念及其面临的安全威胁；然后阐述信息通信技术供应链的安全战略与实践、安全模型与标准规范；接着详细讨论了硬件供应链与软件供应链的安全风险与应对，采办与外包的安全理论及实践；最后分析了我国当前面临的信息通信技术供应链的安全风险，提出了保障我国信息通信技术供应链安全的对策和建议。

本书内容丰富，专业性强，讲解深入透彻，所研究的领域较为前沿，可以作为高等院校信息安全、软件工程、计算机、通信等专业的教学参考书，也可供我国信息技术供应链安全决策者、研究人员及其他相关人员参考。

图书在版编目（CIP）数据

信息通信技术供应链安全/吴世忠等编著.--北京：清华大学出版社，2014
高等学校计算机专业规划教材
ISBN 978-7-302-36418-4

Ⅰ.①信…　Ⅱ.①吴…　Ⅲ.①通信技术－信息产业－供应链管理－研究　Ⅳ.①F49

中国版本图书馆CIP数据核字(2014)第098544号

责任编辑：龙启铭
封面设计：
责任校对：焦丽丽
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**18.5　　**字　　数：**428千字
版　　次：2014年7月第1版　　**印　　次：**2014年7月第1次印刷
印　　数：1～3000
定　　价：　.00元

产品编号：057562-01



前言

信息通信技术供应链是电力、石油石化、核能、航空、铁路、公路、水利、医疗等国家关键基础设施的生命线，对国家安全和国民经济至关重要。随着云计算、物联网、移动互联网的快速普及和广泛应用，一方面信息通信技术已成为现代供应链中不可或缺的组成部分，现代供应链在很大程度上依赖信息通信技术来实现其功能和作用；另一方面信息通信技术本身就是一套完整的供应链，除了关注传统供应链物流层面的安全威胁，更加强调设计、制造、安装、维护、升级等环节的安全风险，以及计算机和通信网络的安全性。显而易见，作为供应链基石的信息通信技术供应链如果不安全，那么所有其他供应链实质上也不安全。

信息通信技术在全世界范围内的发展日新月异，从信息通信技术供应链自身来看，由于其涉及的软硬件漏洞和攻击面日益增加，使得信息通信技术中固有的脆弱性也将随之进入到供应链系统，所以只要有供应链的地方，原则上都有受到破坏的可能；从外部环境来看，目前漏洞挖掘和系统渗透等攻击技术不断智能化，APT 等攻击方法不断创新，攻击人员能力明显提升，使得针对信息通信技术供应链的攻击事件屡见不鲜，而这些事件呈现危害范围广、后果严重、损失巨大等特点。因此，对信息通信技术供应链安全问题的研究已成为当前信息安全工作的重中之重。

信息通信技术供应链的独特性给全世界带来了很多新的安全挑战，而且对该类供应链的攻击将直接威胁国家关键基础设施的安全。因此，确保信息通信技术供应链的安全应作为强化国家信息安全保障的一项基础性工作。面对日益复杂的供应链，全世界，尤其是技术发达、网络化程度高的国家，已逐步开始将信息通信技术供应链安全列入其国家信息安全战略部署并加以实施。其中，美国在其国家网络安全综合计划中将“全球供应链安全”作为第 11 个任务，2012 年又发布全球供应链安全国家战略，通过建立完善的信息产品进出口安全审查机制等一系列措施来保障信息通信技术供应链安全。

与发达国家相比，我国对信息通信技术供应链安全的研究及实践尚处起步阶段，而且亟待完善信息产品安全审查体系等相关措施。因此，开展对国内外信息通信技术供应链安全态势、信息通信技术供应链涉及的具体领域、其他国家的战略和措施等进行系统性研究，有利于提高我国信息通信技术供应链安全保障能力，这也正是撰写本书的出发点。本书运用归纳总结、

逻辑推理与案例研究相结合的方式，对信息通信技术供应链安全威胁、世界各国相关战略、安全模型、相关标准、硬件供应链、软件供应链、采办安全和外包安全等进行研究，并针对我国信息通信技术供应链安全问题提出了探索性的建议。经过三年的调研与撰写，作者编写了本书，以供广大读者学习参考。

本书内容翔实、丰富、专业性强。全书共分为10章，基本内容分为四部分。第一部分包括绪论和信息通信技术供应链面临的威胁两章。绪论主要介绍了信息通信技术供应链相关概念，信息通信技术供应链面临的威胁具体阐述了相关的信息威胁、系统威胁和网络威胁。第二部分是信息通信技术供应链安全态势研究及分析，包含国外供应链安全战略、信息通信技术供应链安全模型和信息通信技术供应链安全标准共三章。从宏观层面讲述了部分发达国家信息通信技术供应链安全战略与实践、主要的供应链安全模型以及目前存在的供应链安全标准等。第三部分是信息通信技术供应链的产品及服务安全。在信息通信技术产品层面，包含硬件供应链安全和软件供应链安全两部分，介绍了硬件和软件供应链安全问题并提出了应对措施；在信息通信技术服务层面，包括采办安全和外包安全，主要阐述了采办和外包的相关理论模型和实践。第四部分针对我国信息通信技术供应链安全面临的严峻形势，专门阐述了我国信息通信技术供应链发展现状，分析了我国当前面临的信息通信技术供应链风险，并根据我国的国情提出了降低供应链风险、保障信息通信技术供应链安全的对策和建议。另外还专门对华为与中兴的案例进行了分析与总结，最后对信息通信技术供应链新技术领域的应用进行了探索研究。

本书的撰写和出版，得到了中国信息安全测评中心的支持和相关实验室的积极配合，得到了国家自然科学基金项目（项目编号：61170273）和中国民航信息通信技术科研基地开放基金项目（项目编号：CAAC-ITRB-201201）的支持。在本书出版之际，由衷感谢国家信息安全各主管部门和社会各界专家和学者的支持、推荐和鼓励。还要感谢北京邮电大学的赵玲玲、许兵、郭晓博、姚普欣、杜士贤、张信媛给予的极大帮助。

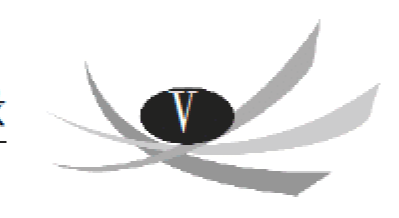
本书编写过程中参阅和研究了许多资料，包括相关领域的国内外著名专家、学者的经典著作和研究论文，主要参考文献已列于每章之后，在此对这些作者表示感谢。

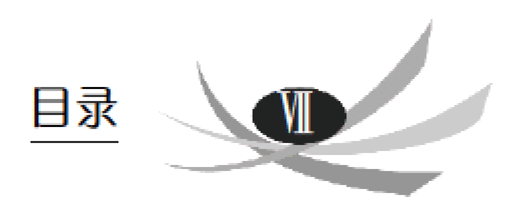
限于作者水平，书中欠妥和纰漏之处在所难免，敬请读者和同行批评指正，联系方式：chendq@itsec.gov.cn，lutb@bupt.edu.cn。

作　者

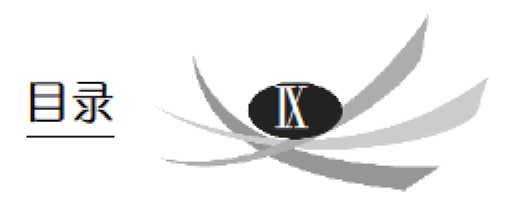
2014年5月


目录


V


Ⅶ

第 10 章 构建我国 ICT 供应链安全 /244



第1章 绪 论

1.1 供应链概念

“供应链”(Supply Chain)的概念产生于20世纪80年代初期。20世纪90年代后期以来,“供应链”成为非常热门的词汇。1963年美国成立的物流管理协会(Council of Logistics Management, CLM),是全球物流和供应链管理领域个人参与的最有影响的行业组织。2005年1月1日,该协会正式更名为美国供应链管理专业协会(Council of Supply Chain Management Professionals,CSCMP),域名也从www.clm1.org更名为www.cscmp.org,这标志着全球物流进入供应链时代。当年,该协会的物流突出贡献奖得主马丁·克里斯托弗有一句名言:“在21世纪,市场竞争将是供应链和供应链的竞争,而不是企业和企业的竞争。”畅销书《世界是平的》曾将供应链列为碾平世界的第七大动力,并以沃尔玛为例详细阐述了供应链的巨大威力[TF2006]。

关于“供应链”一词,存在各种各样的解释。美国供应链管理专业协会2006年10月更新的《供应链与物流术语》的定义是:供应链始于未加工的原材料,终于使用产品的最终用户,供应链将许多企业联结在一起。从原材料的采购到成品送到用户手中的物流过程中实体和信息的交换。所有卖主、服务提供商以及客户在供应链中相互关联[SCLTG2006]。

2012年1月美国《全球供应链安全国家战略》给出的描述是:全球供应链提供食品、医药、能源和产品来支持我们的生活。许多不同的实体负责或者依赖全球供应链,这些实体包括监管部门、执法部门、国营及私营贸易部门和其他国内外合作者。全球供应链系统依赖于运输基础设施、信息通信技术、互联网和能源网络的相互关联。这种关联性能够促进经济活动,然而也会在广泛的地理区域或者产业界引起局部或者区域性破坏传播风险[NSGSCS2012]。

维基百科给出的定义是:供应链是以完成从采购原材料,到制成中间产品及最终产品,然后将最终产品交付用户为功能的、由一系列设施和分布选择形成的网络。

我国国家标准《物流术语》(GB/T-18354-2006)的定义是:生产及流通过程中,涉及将产品和服务提供给最终用户活动的上游与下游企业所形成的网链结构。

随着全球供应链的逐渐发展,供应链安全问题也日益突出起来。为确保供应链的安全,目前世界各个国家及地区纷纷制定了自己的供应链规范。

2003年,美国推出“海关-商业伙伴反恐计划”(Customs-Trade Partnership Against Terrorism,C-TPAT),包括一系列获得广泛认同和支持的要求。C-TPAT目前仍然是美



国最主流的法案，若符合此项要求，在与美国相关的贸易中可获得相关便利。

在美国制定相关规范的同时，国际组织也制定了通用的国际标准，其中包括全球贸易安全与便利标准架构(SAFE)与ISO/PAS 28000标准。

相比于美国和国际组织，欧盟制定的供应链的规范优质企业认证(AEO)和《国际船舶和港口设施保安规则》(International Ship and Port Facility Security Code，ISPS Code或ISPS规则)相对较晚，但这也为制定欧盟的规范提供了更多的参考。

由于经济发展和政治体制的原因，亚洲和大洋洲地区并没有形成较为统一的供应链规范体制。各国呈现“百花齐放，百家争鸣”的景象。亚太地区的供应链规范主要参考C-TPAT和AEO，由于没有统一的规范和完整的体系，不同国家和地区的供应链活动产生了一系列的问题。

在世界各国和地区制定自身供应链规范的同时，企业联盟也同时公布了自己的规范。其中较著名的是TAPA制定的FSR。

在南美及拉丁美洲地区，还存在一个安全商业联盟(BASC)，它是由一家北美公司成立的一个自愿性的组织。BASC的主要参与者是拉丁美洲公司。有人提议引入美国对供应链采取的安全措施，以防范关税风险、走私毒品、盗窃及散发受污染货物等。

1.2 ICT供应链定义

ICT(Information and Communication Technology)通常被称为信息通信技术。ICT是当今世界发展最迅速、渗透最广泛、应用最成熟的新兴技术。2011年12月，美国巴特尔(Battelle)慈善信托基金会发布了《2012全球研发经费预测》报告[GFF2011]，该报告认为过去20年里，ICT已成为许多领域的关键创新因素，并极大地改变了全球范围内的社会行为。表1-1列举了近年来世界部分国家及地区政府部门为促进ICT产业发展所采取的一系列政策或措施。

表1-1 近年部分国家和地区ICT计划

国家和地区	计划或战略	起止年份	主要内容或目标
美国	国家宽带计划	2009	保证在美国人人都有宽带接入
加拿大	扩大宽带接入	2009—2012	投入2.25亿加元用于扩大宽带接入
欧盟	数字化议程	2009—2020	2020年，欧盟至少一半的家庭宽带速率超过100Mbps
英国	数字英国	2009	建设高速光纤网络，全面升级数字广播
法国	数字法国	2009—2020	构建“连接全国居民的宽带网”和“ICT数字支柱产业”；发展固定和移动宽带，推广数字化应用和服务，扶持电子信息企业
德国	数字化德国	2010—2015	促进物联网、服务联网、云计算、3D技术等新技术的研发，改善数字世界的安全与可信度
芬兰	立法保证宽带接入	2010	到2015年年底前，要让至少100Mbps速度的宽带接入成为芬兰人的法定权利

续表

国家和地区	计划或战略	起止年份	主要内容或目标
澳大利亚	光纤进家庭	2009	组建一个全国性高速光纤宽带网络，将耗资434亿澳元
巴西	国家宽带计划	2010—2015	投入57亿美元的资金建设国家宽带
日本	i-Japan战略	2009—2015	发展电子政府和电子地方自治体，推动医疗、健康和教育的电子化
韩国	IT韩国	2009—2013	把信息整合、软件、主力信息、广播通信、互联网5个领域确定为信息核心战略领域
新加坡	智慧国2015计划	2006—2016	高速宽带网将遍布全国
中国	2006—2020年国家信息化发展战略	2006—2020	把信息通信技术的应用和发展作为一个战略议程；加快建设宽带、融合、安全、泛在的下一代国家信息基础设施，推动信息化和工业化深度融合，推进经济社会各领域信息化[GJXX2006]
	国务院关于大力推进信息化发展和切实保障信息安全的若干意见	2012	实施“宽带中国”工程，构建下一代信息基础设施；推动信息化和工业化深度融合；鼓励大中型企业开展网络采购和销售，加强供应链协同运作[GWY2012]
	中国共产党第十八次全国代表大会报告	2012	建设下一代信息基础设施，发展现代信息技术产业体系，健全信息安全保障体系，推进信息网络技术广泛运用
	中共十八届三中全会公报	2013	设立国家安全委员会，完善国家安全体制和国家安全战略，确保国家安全

ICT供应链，包括硬件供应链和软件供应链，通常涵盖采购、开发、外包、集成等环节。其最终的安全很大程度上取决于这些中间环节，涉及到终端用户、政策制定方、采购方、开发方、系统集成方、网络提供方以及软件/硬件供应商等。ICT供应链是所有其他供应链的基础，实际上，它们是“供应链的供应链”。几乎所有的供应链都依赖相互交汇的计算机和通信技术[BAH2012]。

在美国马里兰大学发表的《建立网络供应链保障参考模型》报告中，提出了网络供应链的概念，可以称为ICT供应链的另一种表述形式。网络供应链是指包含于或使用网络基础设施的关键行动者的全部集合，包括终端用户、政策制定者、采购专家、系统集成商、网络提供者以及软件/硬件供应商。这些用户/供应商之间通过组织和过程层互动来计划、构建、管理、维护和保护网络基础设施。与实体供应链相类似，网络供应链是一个端到端的过程。该过程始于软件开发商，其职责与实体供应链上的供应商类似。实体供应链上采购部门、生产和分发管理者的角色与网络供应链上的政策制定者和系统集成商、硬件/组件开发商、软件供应商的角色极其类似。实体供应链上的消费者与网络供应链上的操作者/终端用户相对等[SAICM2009]。

相对于传统领域的供应链，ICT供应链有其特殊性。ICT系统通常是“采购＋开发＋集成”模式，其最终用户感知到的安全很大程度上取决于采购、开发和集成等这些中间环

节，涉及更多的外包方、集成商以及其他第三方等，这些供应商的安全素养、流程和产品质量的重要性愈发地凸显出来。

简要来说，ICT 的供应链的特点包括：使用的设备多，通常包括硬件、软件等众多组件；项目涉及全球很多地区的供应商、生产厂、集成商、运输服务商等；ICT 业界主要依靠采购成熟的商业组件和设备，对供应链的依赖性更强；设备之间有很多通信功能等关联关系；设备的功能和质量很难被完全地测试、测量和直观地展示出来，等等。

ICT 供应链作为特殊的供应链，ICT 供应链风险管理较一般物流供应链风险管理涉及的方面更广，更加复杂，如图 1-1 所示。



图 1-1　ICT 供应链风险管理

1.3　ICT 供应链安全挑战

2011 年 2 月，伊朗突然宣布暂时卸载其首座核电站“布什尔核电站”的核燃料，因为布什尔核电站遭到“震网”病毒攻击，使其 1/5 的离心机报废。事实上，自 2010 年 8 月该核电站启用后就发生连串故障，原因是核电站遭一种名为“震网”(Stuxnet)的蠕虫病毒入侵。该病毒沿着供应链侵入了伊朗工厂企业甚至进入西门子为核电站设计的工业控制软件，并可夺取对一系列核心生产设备尤其是核电设备的关键控制权。整个攻击过程如同科幻电影：由于被病毒感染，核电站的监控录像被篡改。监控人员看到的是正常画面，而实际上离心机在失控情况下不断加速而最终损毁。

震网的攻击载体直指西门子公司的 SIMATIC WinCC 系统。这是一款数据采集与监视控制(SCADA)系统，被广泛用于钢铁、汽车、电力、运输、水利、化工、石油等核心工业领域，特别是国家基础设施工程。该系统运行于 Windows 平台，常被部署在与外界隔离的专用局域网中。震网病毒之所以能够成功进入伊朗核电站与外界隔离的专用网中，并

不是通过人们常见的互联网，而是利用了 ICT 供应链的漏洞，提前被植入系统中。

此后，伊朗还曾发现一种名为“毒区(Duqu)”的数据窃取病毒，针对的也是工业控制系统，但它并没有危害伊朗核能实验室和工业设施内的电脑。

2012 年 5 月，国际电信联盟和多家电脑安全公司宣布，一种名为“火焰”的破坏力巨大的全新电脑恶意软件被发现，它是迄今为止世界上最复杂的计算机病毒。俄罗斯 IT 安全公司卡巴斯基实验室在当天的报告中说，“火焰”已侵入伊朗、以色列、巴勒斯坦、叙利亚、黎巴嫩和沙特等中东国家数百台电脑，全球受感染电脑估计在 1000～5000 台之间。

该消息随即得到伊朗方面的证实。该国官员称，“火焰”曾侵入伊朗一些行业的电脑，“所幸被及时发现”。该病毒企图收集伊朗石油行业的关键信息，曾在今年 4 月份对伊朗石油网络系统造成影响，导致当局短暂切断石油部、石油出口数据中心等机构与互联网的连接。

2012 年 5 月，美国参议院军事委员会(Senate Armed Services Committee)发布报告称，历时一年的调查发现，在 2009—2010 年间，美国国防部供应链中共发生 1800 起假冒零部件事件[SASC2012]。美国空军 C-130J 运输机采用了假冒电子零件，特种行动直升机和海军的“海神”(Poseidon)侦察机的组件中也有假冒电子零件。报告称：“一个电子部件的失灵可能导致士兵、海员、飞行员或海军陆战队在危急关头命悬一线。”“不幸的是，大量假冒电子部件明显加大了安全预防工作的难度。”除影响国家安全并造成安全风险外，假冒电子部件还增加了系统成本。以美国导弹防御局一个导弹为例，更换其中一个假冒存储设备的成本便高达 270 万美元。

2013 年 1 月 7 日至 16 日，在短短的 10 天之内，美国波音 787“梦想飞机”就出现了 7 次程度不同的事故，引发了人们对其安全性的强烈质疑。随后，美国、日本、波兰、卡塔尔、印度、智利、埃塞俄比亚等国家的 8 家航空公司全部宣布停飞 787 客机。专家指出，波音 787 客机连发电瓶起火、燃油泄漏、刹车故障、驾驶舱玻璃裂缝、飞机连接线等故障，其背后可能是全球“碎片化”供应链制造模式惹的祸，这给飞机制造的质量管控带来了严峻挑战。787 客机采用外包制造，大部分零部件供应商分布在全球各地，有媒体称欧航高管认为波音把技术用到极限，外包也用到了极限。波音出于降低成本的考虑将模块外包时埋下了隐患，模块承包商势必也将自己的任务进一步分解外包，依此类推，直至产品细化到一个铆钉。一级承包商以下的工作是波音公司无法控制的，所以当下面任何次一级生产出现问题的时候，就像推倒了多米诺骨牌，导致整个飞机出现故障。

众多特点给 ICT 供应链来了很多新的威胁与挑战。从软件工程过程中出现的软件缺陷，到供应商内部的恶意人员，到可能的商业间谍甚至国家网络战等各种各样的威胁，针对目标的供应链的攻击已成为攻击其 ICT 系统的一个重要路径。

ICT 供应链的实际活动开始于采购，但是很少有采购系统可以在供应链中完整地跟踪最终产品，不管它是制造电子部件的原材料，由电子部件装配而来的电路板，还是构成一个子系统的电子部件均是如此。大多数的项目办公室、制造商和供应商都视自己的责任为：从他们的供应者那些获得物资、实施他们负责的行动(合同的或者官方的)、向供应链的下一阶段传送产品。

当事者通常不会考虑全球性的系统评估，只看眼前的工作：部件只要能简单地工作，

表现符合预期就可以了。制造硅片的制造商通常并不了解,或者真正关心,这些硅片正在进入一种低能的雷达放大器或者一种高速计算机当中,只要这些硅片通过了工厂的验收测试就可以了。至于一箱硅片在高速公路上无人防守地停留了三周的时间,制造商是没有兴趣去关心的。只要这些硅片在合同规模的交付时期内抵达到了供应链中下一级生产商手里,硅片制造商及其用户都是满意的。

采购或者外包是ICT供应链管理中非常重要的环节,在这些环节中,供应链本身可能会被敌人利用来传送威胁或者发动攻击。目前,随着采购和外包商用现成品技术的推广应用,以及开源软件产品的增加,终端用户寻找机会来重新配置或者做一些有限制的增加方法来安装软件和系统,这些因素都增加了对供应链安全风险的忧虑。所有的软件几乎都有缺陷,一般的缺陷可以很容易的被未授权的组织发现,进而为其恶意的目的更改产品的安全属性和软件的机能。这些缺陷可以是在软件开发或者使用期间,被故意插入到软件中。随后的采购者和用户很难发现和改正这些缺陷并避免被其利用。不怀好意的攻击者会感染供应链,他们会向产品和服务中插入允许某个实体控制其他组织的信息和通信技术系统的功能,可能是为了盗取信息、更改信息或在重要时刻拒绝服务。应该从供应链的最开始,就对产品进行完整的跟踪,在每一个点上反复实施适当的控制,以确保产品在整个供应链中的安全性。

由于互联网技术的发展和普及,供应链上相关ICT产品中也存在无数脆弱的链接。攻击者常常将供应链作为攻击中首要的部分。攻击的目标可能包括硬件、软件、国际互联网结构或者包括那些由移动装置使用的通信基础设施中的弱点。

不仅如此,应该说供应链的所有方面都可能遭受网络攻击或者操控,包括设计、制造、传输和运送、安装、维护或者升级。敌人可以利用执行攻击的操控的途径数量众多。几乎所有的供应链都依赖相互交汇的计算机和通信技术。如果计算机和通信被破坏了,那么所有供应链就被破坏,不管人们是否已经知道受到了攻击。此外,因为计算机和通信技术在全世界范围内实现了更新换代,所以只要有供应链的地方,原则上都会受到破坏。现在,全世界范围内的供应链用户缺乏必要的硬件或者软件安全技术和业务程序,不能获得更好的安全环境。

美国问责办公室(U. S. Government Accountability Office,GAO)表示,政府的IT供应链威胁包括软硬件上的恶意逻辑、假冒软硬件的安装、生产过程或是重要产品或服务的分销过程中出现问题、因技术性能问题而依赖于不合格的服务供应商,以及软硬件上无意中安装的漏洞等等。

ICT供应链的攻击者可能会搞破坏活动,恶意引入不需要的功能来破坏系统的设计、完整性以及制造、生产、分发、安装、运营或维护过程,以便进行操作或拒绝访问、扰乱或降低其可靠性和可信赖性。ICT供应链面临的威胁以系统失灵、拒绝服务、欺骗伪装、破坏或者盗取数据、物资失窃、传输延迟以及误导式的服务体现出来。它们可以是很明显、即时发现的事件;可以是在未来特定的事件发生的时候才生效的后门;也可以是定在未来某个时刻发生的事件。这些威胁不仅会破坏物资和服务的流动,而且会破坏整个供应链网络,最终影响企业的发展,甚至影响国家安全。

在我国,ICT高速发展的同时面临的供应链安全问题也十分严峻:对外国的严重技

术依赖,已成了我国建设经济强国的最大、最现实危机。据中国海关总署统计,2009年,我国单项商品进口中,进口石油花了900亿美元,铁矿石进口花了500亿美元,而芯片进口价值达1200亿美元,大尺寸电视液晶面板进口达400亿美元[中国海关总署进出口统计年度报告2009]。

中科院院士、材料学家邹世昌介绍,目前中国集成电路芯片80%依靠进口,在这方面消耗的外汇超过石油,成为第一外汇消耗大户。“缺乏核心竞争力是中国相关产业的硬伤。中国集成电路工艺技术较国际先进水平差距不小。要缩小差距,还需要在核心技术上取得突破。”

1.4　本书内容和框架结构

围绕信息通信技术供应链安全,可将本书内容组织为四个部分,如图1-2所示。



图本书结构图

第一部分:第1章和第2章为ICT供应链安全概述,介绍ICT供应链相关概念以及面临的威胁。

第二部分和第三部分从宏观和微观两方面阐述ICT供应链安全。第二部分为ICT供应链安全态势研究及分析,从宏观层面讲了国际上ICT供应链安全战略、供应链安全模型以及供应链安全标准。

第三部分ICT供应链产品及服务安全,分别从ICT产品(即硬件、软件)和ICT服务(采办、外包)几个方面阐述供应链安全。

第四部分:对我国ICT供应链安全提出了建议。

第1章为绪论,介绍供应链、ICT以及ICT供应链的相关概念和发展状况,以使读者对ICT供应链形成初步概念,随后引出本书的主题:ICT供应链安全。

第2章ICT供应链面临的安全威胁,分析供应链信息威胁、供应链系统性威胁以及网络威胁等,阐述了网络威胁的不对称特性,指出它是少数人对多数人犯下的罪行,几乎不需要成本,却能造成很难预测的影响。最后从宏观上介绍了ICT供应链网络威胁的应对策略。

基于ICT供应链网络威胁产生了世界范围的影响,引起了越来越广泛的重视。世界上许多国家都开始对此发布了有利于自身的安全战略并逐步付诸实践。第3章国外ICT供应链安全战略,从细节上介绍各个国家的ICT供应链安全战略与实践历程,并对部分国家的战略进行了简要分析。美国和欧盟在ICT供应链安全方面一直走在世界前列,故而首先从美国和欧洲讲起。而一些发达国家因ICT供应链安全研究起步较晚,尚未出台明确的ICT供应链安全战略,因此本书只分析了该国制定的相关安全战略。章末则对各国战略的异同做了简要的分析。

第4章供应链安全模型,将重点锁定在供应链安全模型的实现上,总结了国际上最新的供应链安全模型并阐述了各个模型在保护ICT供应链安全领域的应用,包括供应链运

作参考模型、供应链安全确保模型、供应链安全控件模型、NIST 系统开发生命周期模型、达沃斯-供应链和运输风险模型、ICT 供应链集群框架，为相关组织机构提供了 ICT 供应链风险管理的工具。

第 5 章供应链安全标准，介绍与 ICT 供应链相关的国际标准或一些国家制定的国家标准。主要有 ISO 28000 供应链安全管理体系、ISO 27036 网络供应链风险管理指南、ISO 15026 系统如软件确保标准等。本书从各个标准产生的背景、内容与发布后的意义等方面对其进行了详细的分析，以供有需求的读者参考。

硬件供应链和软件供应链是 ICT 供应链的重要组成部分，也是安全威胁的主要来源。第 6、7 两章主要论述了硬件供应链安全和软件供应链的安全。硬件供应链安全部分探讨了硬件供应链目前所面临的风险，如硬件木马、仿冒和伪造等。软件供应链安全部分分析了软件供应链面临的特殊威胁。为应对这些威胁，文章从供应链完整性角度提出了软件供应链确保的概念，介绍了 5 种软件供应链安全确保模型。

第 8、9 章从 ICT 供应链服务的角度切入，重点讲解 ICT 供应链中的采办和外包安全。采办安全部分介绍了当今常见的采办框架，接着举出了采办安全风险以及相应对策。外包安全部分阐述了外包的基本理论、安全模型、安全风险以及风险管理方法。

针对我国 ICT 供应链安全的严峻形势，本书的第 10 章专门阐述我国 ICT 供应链发展现状，分析我国当前面临的 ICT 供应链风险，并根据我国的国情提出了一些降低供应链风险、保障 ICT 供应链安全的对策和建议，以供国内企业和组织参考。

参 考 文 献

[BHA2012] Booz Allen Hamilton. Managing Risk in Global ICT Supply Chain: Best Practices and Standards for Acquiring ICT. 2012.

[BJPSCSI2006] B. Johnson. Port and Supply-Chain Security Initiatives in the United States and Abroad. 2006.

[EFNMASC2012] World Economic Forum. New Models for Addressing Supply Chain and Transport Risk. 2012.

[GFF2012] Battelle. 2012 Global R&D Funding Forecast. 2011.

[SAICM2009] Developing a Cyber Supply Chain Assurance Reference Model. 2009.

[LR2011] LOGSEC. The LOGSEC Roadmap. 2011.

[NEIII2004] NIST. Economic Impact of Inadequate Infrastructure for Supply Chain Integration. 2004.

[PYSWL2011] Pwc. 运输和物流 2030 卷四：保障供应链安全. 2011.

[SCSG2009] The Worldbank, Supply Chain Security Guide. 2009.

[SCSITFP2008] The Swedish National Board of Trade. Supply Chain Security Initiatives: A Trade Facilitation Perspective. 2008.

[USNSGSC2012] The White House. US National Strategy for Global Supply Chain Security. Janurary 2012.

[ZNRI2008] Zlatko NEDELKO. The Role of Information and Communication Technology in Supply Chain. 2008.

[SASC2012] Senate Armed Services Committee. Senate Armed Services Committee Releases Report on

Counterfeit Electronic Parts. 2012.
[ZGHG2009] 中国海关总署.中国海关总署进出口统计年度报告. 2009.
[GJXX2006] 国家信息化领导小组. 2006—2020 年国家信息化发展战略. 2006.
[GWY2012] 国务院关于大力推进信息化发展和切实保障信息安全的若干意见. 2012.

第2章

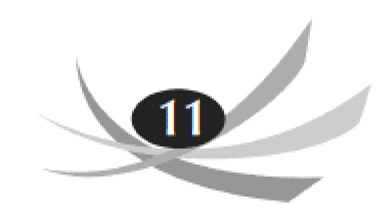
ICT 供应链面临的威胁

2.1 概　　述

信息通信技术(ICT)包括用于收集、存储、传递、检索或者信息处理的所有技术种类,包括微电子、印刷电路板、计算系统、软件、信号处理机、移动电话、卫星通信和网络,可以是一个独立的成分,例如软件应用或者内存芯片、单机商品(笔记本电脑),也可以是更大系统的一部分(喷气式飞机的航空电子设备)。ICT 是现代文明的命脉,组织和个人都依赖 ICT 来支持关键活动和任务的实施,集成了复杂的全球分布的 ICT 供应链网络,如图 2-1。ICT 供应链整合了跨越多个大洲的多个级别的供应商并生产各种相关产品,从传统的 ICT 产品(例如,服务器、路由器、移动设备)到专门产品组件、遗留系统和备件。这



图 2-1　复杂的 ICT 供应链[BAH2012]



些供应链中的角色从系统集成者到软件开发商、硬件制造商(例如,芯片和其他逻辑组件)和媒体存储处理提供商,覆盖了链中各个环节。

多样化全球 ICT 供应链——从设计和采购到集成、操作、维护和处理——提供了很多节约成本和灵活性的可能性,同时也引入了风险,为攻击者破坏 ICT 基础设施提供了可能性。供应链的所有方面都可能遭受网络攻击或者操控,包括设计、制造、传输和运送、安装、维护或者升级,攻击者可以通过引入恶意逻辑、伪造组件来破坏系统的可靠性、可用性、完整性,或者通过阻断供应链关键产品的供应来迫使供应链中断,这些攻击都可以在制造、生产、分发、安装、运营或维护过程中被攻击者渗透进入供应链。ICT 供应链面临的威胁以系统失灵、拒绝服务、欺骗伪装、破坏或者盗取数据、物资失窃、传输延迟以及误导式的服务体现出来。它们可以是很明显、即时发现的事件,可以是在未来特定的事件发生时才生效的后门,也可以是特定的在未来某个时刻发生的事件。这些威胁不仅会破坏物资和服务的流动,而且会破坏整个供应链网络。ICT 供应链是与所有其他供应链共用的一种东西,它实际上是“供应链的供应链”。如果 ICT 供应链被破坏了,那么依赖 ICT 技术的所有供应链就被破坏,不管人们是否已经受到了攻击。由于 ICT 在全世界范围内的应用普及,只要有供应链的地方,原则上都可能受到破坏。而且全世界范围内的供应链用户缺乏必要的硬件或者软件安全技术和业务程序,不能获得更好的安全环境[CU2010]。

ICT 供应链安全问题可能会威胁到国家安全,破坏和削弱政府保护其民众安全的能力。攻击者通过攻击关键系统和政府的功能来直接摧毁社会,这些攻击可以阻止军队与战斗区域内单位通讯的能力,或者影响依赖特定远程资产的一次性攻击能力。攻击者也可以通过操控或者利用各类信息,来破坏公民、其他政府和非政府组织对本国政府的信任。这样的攻击可以破坏或者颠覆与威胁信息相关的例行规划。攻击者还可以通过对不太重要的功能进行分散式的攻击来影响社会的士气。因此,政府必须要确立有效的计划和程序来反制 ICT 供应链威胁[CU2010]。

2.2 ICT 供应链信息威胁

221 信息共享的威胁

“在现代世界,供应链就是信息。当某些东西被订购的时候……将在哪里生产、由谁生产、生产多少、具体规模是多少……所有的信息到达国际互联网上或者进入私人数据系统中,都有可能会被拦截和入侵。”——前弗吉尼亚州州长詹姆斯·S·吉尔莫(James S. Gilmore, III)

21 世纪的竞争是供应链之间的竞争,用户消费个性化需求的增长,市场对产品多样化要求的提高,经济多样性的升级等,促使企业越来越注重供应链的协调与协同运作。供应链管理把供应商、生产厂家、分销商和零售商等在一条供应链上的所有节点企业都联系起来并对其相互之间的运作环节进行优化,供应链的所有节点企业基于共同的目标,借助于信息技术而组成了一个核心能力的集成体“动态联盟”,组织内的成员通过信息(供应链中的信息包括了所有供应链节点企业之间相互传递的销售信息、采购信息、库存信息、制

造信息和技术进步信息等)的共享,能够协同快速地响应市场需求,优化组织目标。

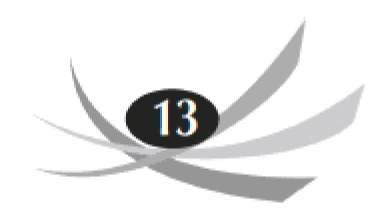
信息共享不仅可以帮助供应链上的企业更好的安排生产作业及库存配送计划,降低供应链的整体成本,还能促进合作企业间的相互信任,加快供应链整体对市场变化的响应,它可以节省时间和提高企业信息交换的准确性,减少复杂、重复工作中的人为错误,从而减少由于失误而导致的时间浪费和经济损失,提高供应链管理的运行效率[DXT2009]。在信息社会中,企业能否在激烈的市场竞争中生存和发展,关键是要看企业能不能及时有效地获得生产经营管理中所需的各种信息。企业要建立快速反应(Quick Response,QR)策略,实现风险共享、提高服务水平等目的,以使企业能更好地面对竞争激烈、快速变化、不确定因素增多的市场。ICT 在 QR 策略中担任了不可替代的角色[YZG2011]。

供应链信息共享是提高供应链协同管理效率和整体绩效的有效途径,然而在供应链协同管理实际运行中,信息共享面临着各种威胁,主要有以下 3 种:一是供应链节点企业追求自身利益最大化,担心其核心技术、采购、销售、财务等商业机密信息外泄,或担心无利可图、增加信息管理成本、个别企业诚信缺失等原因,从而导致节点企业隐匿、提供不完整信息,非核心节点企业缺乏长远考虑因而在信息共享方面往往缺乏主动性,因运营成本较高导致信息共享程度低下。二是供应链共享信息标准化问题有待解决,多数行业之间缺乏统一的信息化技术标准与服务规范,使供应链在不同行业的企业之间,很难找到统一的行业标准,加之缺乏规范非标准化信息的支持手段,以上问题的存在,客观上加大了我国企业供应链信息共享的难度;三是供应链节点企业信息管理水平参差不齐,导致信息共享受阻[LC2012]。信息在供应链节点间进行传送时,可能出现信息失真、信息阻塞、信息不及时、不完善等情况,这将造成节点企业获得信息的不对称,导致供应链通向市场的实际情况和预期之间存在偏差,从而使实际生产计划和实际市场需求状况之间出现偏差,这种偏差会随着供应链的增长而累积得越来越大,最后可能造成节点企业的重大损失,所以信息共享对供应链的正常运作至关重要。供应链中的节点越多、长度越长,信息就越难以实现共享。

222 信息泄露的威胁

所谓供应链信息泄露是指在供应链的信息共享过程中,共享的信息被有意或无意地泄露给没有参与信息共享的其他企业的过程。这里所说的没有参与共享的其他企业,既包括供应链上没有参与信息共享的成员企业,也包括供应链之外的企业。供应链信息主要通过以下 4 种途径泄露[DXT2009]。

(1) 独立于供应链之外的第三方企业泄露信息。在供应链中,企业往往需要和第三方信息收集公司共享信息以便于更好的把握市场状况并进行决策。但是,掌握了供应链成员的信息以后很容易引发第三方信息收集公司的败德行为,比如有一些信息收集公司会将自己掌握的信息标价出售给共享信息企业的竞争对手。[DXT2009]2001 年 Wal-Mart 宣布不再和 Information Resources Inc. 和 ACNielsen 等第三方信息收集公司共享销售数据,原因是这些公司将共享销售信息出售给了 Wal-Mart 的竞争对手,给 Wal-Mart 造成了严重的经济损失[HCL2004]。



(2) 供应链上游企业泄露信息。供应链的信息共享通常是指下游企业将信息和上游企业共享,下游零售商将其掌握的市场需求信息传递给上游制造商与之共享。但是,这也增加了零售商共享给制造商的信息被泄露的可能。因为将共享信息泄露给下游零售商可以提高制造商对市场需求预测的精度,从而使制造商的产量更加接近于市场需求的真实水平,这样就会减少因缺货或者库存而产生的成本。因此,为了提高收益制造商往往会将共享的信息主动或者有意的泄露给没有参与共享的企业。由于泄露信息可以提高自己的收益,制造商往往是无偿披露零售商共享的信息[DXT2009]。

(3) 供应链下游企业泄露信息。在供应链中上游企业将产品出售给下游企业也往往会导致信息泄露。出售给下游企业产品包含了上游制造商的很多创新技术,下游企业购买产品后为了促进上游企业之间的竞争以便获得更低廉的采购价格,往往会将产品中的创新技术故意泄露给其他上游企业[DXT2009]。

20 世纪 90 年代,GM 公司在没有得到许可的情况下将供应商的产品创新泄露给其他的供应商,以获得更低的采购价格,从而达到节约成本的目的。在 Ward 2007 年的一项针对 447 个汽车零配件供应商进行的关于产品创新的调查中,有超过 28%的汽车零件供应商反应其知识产权至少被一家汽车制造商泄露过[MT2007]。

(4) 供应链管理系统泄露信息。供应链是一个极其复杂的信息管理系统,尤其当它发展到集成供应链的阶段时,要靠计算机网络来传输和承载大量的数据。除了少数的信息安全要求特别高的供应链网络采用专网以外,绝大多数供应链是基于 Internet 网络体系构建的。Internet 技术的引入,使得供应链上各个节点企业之间进行高质量的信息传递和信息共享成为可能。带来便利的同时,网络环境的开放性使供应链企业在利用 Internet 进行信息共享的过程中不可避免的带来了信息泄露的隐患。在供应链信息共享过程中信息可能要通过多个网络设备,从这些网络设备上都能不同程度地截获信息的内容,这样就增加了信息泄露的可能。竞争对手或商业间谍可能从 Internet 入侵企业内网,得到企业的私有信息,从而在市场竞争中获得主动。黑客也可以发起针对供应链网络服务器的攻击,给企业造成巨大的损失。在供应链的网络信息安全问题中,数据库的安全问题尤其需要格外重视,由于供应链中的各个企业往往需要共享库存信息、需求信息、销售信息、预测信息、客户资料和技术文档等信息,这些对各个企业及整个供应链至关重要的共享信息被大量的存储于数据库中,如果数据库遭受攻击,则供应链上所有的企业都将受到影响,如果数据库内的信息被无意或有意篡改,同样这些企业将无法进行正常的经营活动[DXT2009]。

2.3 ICT 供应链系统威胁

随着网络空间(Cyberspace)的迅猛发展,以及经济全球化的逐渐深入,ICT 供应链的长度、复杂度、地理分布都大幅增长。ICT 供应链由硬件供应链和软件供应链组成,通常涵盖采购、开发、外包、集成等环节。其最终的安全很大程度上取决于这些中间环节,涉及到终端用户、政策制定方、采购方、开发方、系统集成方、网络提供方以及软硬件供应商等。

ICT 供应链的实际活动开始于采购,但是很少有采购系统可以在供应链中完整地跟

踪最终产品，不管它是制造电子部件的原材料、由电子部件装配而来的电路板，还是构成一个子系统的电子部件。在ICT硬件供应链中，大多数的项目办公室、制造商和供应商都视自己的责任为：从他们的供应者那里获得物资、实施他们负责的行动（合同的或者官方的）、向供应链的下一阶段传送产品。当事者通常不会考虑全球性的系统评估，只看眼前的工作：部件只要简单地工作，表现符合预期就可以了。制造硅片的制造商通常并不了解或者真正关心这些硅片正在进入一种低能的雷达放大器或者一种高速计算机当中，只要这些硅片通过了工厂的验收测试就可以了。至于一箱硅片在高速公路上无人防守地停留了三周的时间，制造商是没有兴趣去关心的。只要这些硅片在合同规定的交付期内到达供应链中下一级生产商手里，硅片制造商及其用户都是满意的。ICT软件供应链中，谁接触到哪些具体的产品或者服务，对于供应链中的其他人来说是不可见的。通常的情况是，一个收购商，比如国防部（DoD）计划办公室，其仅仅了解与他直接联系的参与者，而对供应链中的次级供应商一无所知。任何一个次级供应商都可以插入缺陷，在以后伺机破坏。这样就形成了供应链的安全漏洞，带来了巨大的系统威胁［CU2010］。

采购或者外包是ICT供应链管理中非常重要的环节，在这些环节中，供应链本身可能会被敌人利用来传送威胁或者发动攻击。目前，随着采购和外包商用现成品技术的推广应用，以及开源软件产品的增加，终端用户寻找机会来重新配置或者做一些有限制的增加方法来安装软件和系统，这些因素都增加了ICT供应链系统威胁。所有的软件几乎都有缺陷，一般的缺陷可以很容易的被未授权的组织发现，进而为其恶意的目的更改产品的安全属性和软件的机能。这些缺陷可以是在软件开发或者使用期间，被故意插入到软件中。随后的采购者和用户很难发现和改正这些缺陷以避免被其利用。攻击者会通过这种方式感染供应链，向产品和服务中插入允许某个实体控制其他组织的ICT系统的功能，以便盗取信息、更改信息或在重要时刻使系统拒绝服务。应该从供应链的最开始，就对产品进行完整的跟踪，在每一个点上反复实施适当的控制，以确保产品在整个供应链中的安全性［NYM2011］。

2.3.1 恶意逻辑的嵌入

威胁行为者在系统开发和实现过程中可以利用ICT供应链通过篡改来插入包含恶意逻辑的硬件或软件。恶意逻辑是指带有恶意目的故意在系统中包含或植入硬件、固件或软件。例如，病毒和木马是恶意逻辑的两种形式，都可以沿着供应链侵入系统。病毒是指可以自我复制并在未经使用者授权或知情的情况下感染计算机的一种计算机程序。木马指表面上拥有有用的功能但却包含避开安全机制的隐藏的或潜在的恶意功能的一种计算机程序，有时也通过系统实体的合法授权调用程序。恶意逻辑允许攻击者控制整个系统，如阅读、修改或删除敏感信息，中断运行，发起对其他组织的系统的攻击，甚至毁坏系统，导致重大损失。“逻辑炸弹”、“后门”和“间谍软件”在微芯片和电路逻辑、固件和软件中的插入可以破坏或颠覆所供应的零部件［USGAO2012］。

每天都有很多未知病毒和木马潜入ICT供应链，其对ICT供应链造成的危害也愈发巨大。假如一种未知的非常强大的病毒感染了大量ICT系统，它可能会导致大规模的系统故障，进而可能关闭整个范围内的自动化流程，甚至瘫痪整个ICT供应链。如果此类

病毒感染了依靠 ICT 系统保持业务正常运行的运输和物流供应链,这种损失将无法估量。

在集成电路的设计中还有可能植入被称为硬件木马的恶意电路,这是一种植入电子系统的恶意电路模块,通过改变系统功能以达到监控、直至打击对手或潜在对手的目的。硬件木马极为隐蔽、难以发现,只在特定时机才被以特定的方法激活,而在未激活的情况下系统将表现得完全正常,但是硬件木马一旦激活其危害极为巨大。

固件是固化在永久存储器件中的二进制程序,负责控制和协调集成电路,随着集成电路制造技术的发展,固件与传统的应用软件一样,都有可能存在木马、后门、逻辑炸弹等具有恶意行为的代码。电子组件供应链,包括微芯片,可能在某个阶段被敌对代理渗入。这些敌对代理可更改电子组件的电路或用更改的电路替换伪造组件。更换的电路可能包含"恶意固件",它以同恶意软件一样的方式运行。

2.3.2　伪造组件的安装

组件是组装在一起形成一个功能单元的一组元件。伪造组件是包含假冒零部件或代码的硬件或软件。一个组件如果未经授权,不符合设计、模型或性能标准,不是由原始组件制造商生产或由未授权的承包商生产,属于残次品或原制造商以旧充新,拥有错误或假冒的标签或说明书,那么它就是伪造的[USGAO2012]。

出于成本的考虑驱使组织做出获取廉价部件的决定,这将不可信供应商提供低质量的退化更快的部件。一些供应商故意用不符合标准的伪造产品来涌入市场。由于政府监管以及产业本身的漏洞,伪造电子元器件越来越泛滥,短缺部件成为伪造商的目标,造假者准确地掌握着部件市场的情况。他们特别瞄准的目标是需求紧迫并处于缺货状态的产品。设备厂商一般会通过正规销售商来采购半导体及电子部件,但为能按计划生产,采购部件的设备厂商会从部件商及网络销售商等"开放市场"寻找短缺部件,这时就会面临买到伪造产品的威胁[WZ1]。

伪造组件威胁着供应链系统的完整性、可信性和可靠性:伪造品的可靠性通常较低,所以比正品出故障的时间更早而且故障更频繁;伪造给造假者提供了向副本中植入恶意逻辑或后门的机会,而在正品的制造中很难实现。伪造产品可能危及消费者的健康甚至生命;伪造器件对航空航天和国防领域、政府、公民和国家安全造成威胁;仿冒品中有的是以谍报活动和恐怖主义为目的,这种伪造部件一旦被植入系统中,就会像"特洛伊木马"一样收集特定信息或使系统瘫痪,对国家安全系统和金融系统造成巨大威胁。

以美国为例,VisionTech Components 电子器件公司在 2006 年 12 月到 2010 年 9 月间进口的 3263 批次芯片中,只有 35 批在边境被美国海关人员查出含有伪造产品并被没收。未被查出的 3228 批产品被 VisionTech 出售给了 1100 多个来自几乎各个行业的买家,流入了美国电子产品供应链。其中很多买家也是中间供应商,他们将产品再次出售给了其他买主。一部分伪造产品在生产测试过程中被查出,但成千上万的伪造产品可能仍然在供应链中流通,甚至有可能正用于现在的设备中,这种行为可能对美国军队、军人、政府等所有购买其伪造产品的行业和消费者造成不可预测的破坏和伤害[WZ2]。

2.3.3 关键产品的中断

关键产品的中断，即意外事件的突然发生导致供货量与客户需求量、成本或质量与供应链预定管理目标显著偏离。这个定义既包含引发供应链中断的直接或外在原因——意外事件，同时又指出了供应链中断的表现形式——数量、质量或成本与预定管理目标的显著偏离[GPL2011]。关键产品的生产和分配的中断，会影响支撑 ICT 供应链系统的设备的供应。人为的(如由劳动力或政治争论造成的中断)和自然的(如地震、火灾、洪水或台风)都会中断对于机构运营非常重要的 ICT 产品的供应[USGAO2012]。

2011 年 3 月 11 日，日本爆发 9.0 级地震并引发海啸。海啸不仅造成日本经济的惨重损失，也引发了世界 ICT 供应链的“地震”。如图 2-2 所示，汽车、半导体、电子消费品、化工产品及钢材等众多产业受地震严重影响，供应链中断，相关原材料和零部件价格出现不同程度的上涨。日本为 ICT 供应链上游材料及关键零组件的主要供应国，全球大约 40%的内存是由日本制造的，遇及不可抗力因素后短期难以寻得替代供货商，此次地震影响了全球市场计算机内存的供应，造成全球 ICT 产业供应链的巨大缺口[ZX2012]。

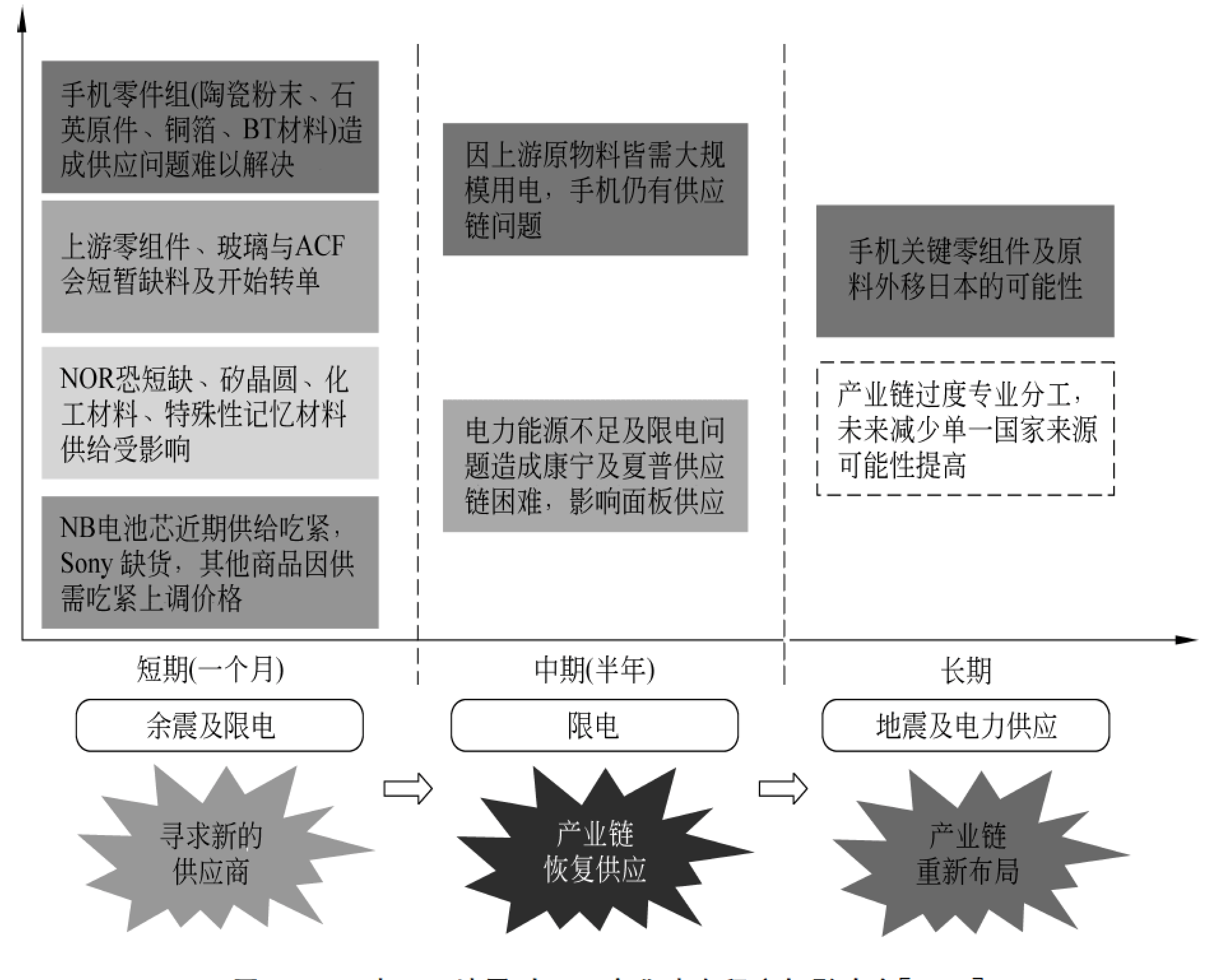
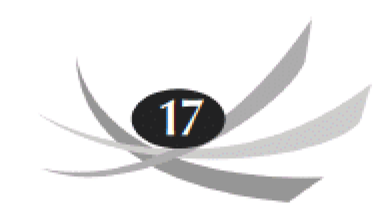


图 2-2　日本 311 地震对 ICT 产业冲击程度与影响力[WZ3]

来源：拓扑产业研究所 2011/03

泰国是仅次于中国的全球第二大硬盘生产国，在全球总产量中占到近一半。2011 年 7 月，泰国遭遇 50 年来最严重的洪灾，使得当地的硬盘生产厂关闭数月之久。通常个人电脑厂商的库存平均可支持四到六周，在库存耗尽后，企业将感受到更加明显的供应链中断冲击。国际知名硬盘厂商西部数据在泰国的产量占其全球产量的 60%。水灾导致硬盘供应短缺，英特尔、苹果和戴尔的业务都不可避免地大受影响。此外，由于索尼公司在



泰国灾区的部分工厂停止生产,该公司推迟发布多款数码相机。泰国的翻天浊浪,将全球供应链体系无情冲断和破坏[WZ3]。

突发事件导致的供应链中断的案例已不鲜见,应该对突发事件导致的供应链中断给予足够的重视。

2.3.4　过旧组件的替换

由于技术进步或者业务优先级的变化,供应商会选择停止某些硬件和软件的生产。而系统的使用期明显长于它的组件的使用期,这使得系统所有者必须找到替换组件的对应替代来源,一些未经授权的承包人和其他服务提供商便会乘虚而入,他们可能会利用其地位的优势,拥有访问数据与系统的权限,从而获得敏感信息、犯罪欺诈、扰乱运营,或对其他系统和网络发动攻击。除非系统拥有者选择执行昂贵的升级或者替换系统,否则他们不得不面临这种组件替换需求造成的威胁,美国国防和航空航天部门称这种现象为减少的生产资源和材料短缺(Diminishing Manufacturing Sources and Material Shortages,DMSMS) [USGAO2012]。

2.3.5　无意漏洞的渗透

无意漏洞是指由于疏忽而插入系统中的可能造成破坏的硬件、软件或固件,它们都是从无意的行为中产生的,例如在软件编码中忽视了由于不充分的硬件测试造成的故障,含有缺陷的组件的插入会对系统运行和集成造成重大威胁。攻击者总是专注于寻找和探索代码中现存的缺陷,如缓冲区溢出,利用这些无意漏洞,攻击者会进行相关操作进行攻击,威胁组织甚至国家的安全,例如美国国土安全部最近发布工业控制系统中的固件中存在已识别漏洞的警报[USGAO2012]。

2.4　ICT 供应链网络威胁

当今时代,ICT 技术在日新月异、突飞猛进地向前发展,把全球的经济、文化联结在一起。任何一个新的发现、新的产品、新的思想、新的概念都可以立即通过先进的 ICT 技术传遍全世界。在企业管理过程中,ICT 供应链已经被视为提高企业生产效率和获得竞争优势的主要来源。如何利用它重组和优化供应链,降低运作成本,提高客户服务水平和整条供应链的竞争能力对于企业来说将是一个刻不容缓的问题 [WZ4]。

2.4.1　网络威胁的产生

供应链是一个包括组织、人员、程序、技术、信息和资源在内的系统。这个系统推动供应商将原材料和自然资源经过生产形成产品,然后将他们的货物输送给用户。在从原材料到制成品的端对端的程序中,供应链的每一步上都面临着持续的威胁。国际互联网的全球到达,政府和非政府网络无处不在的联结使国家暴露各种网络攻击的威胁之下。任何的信息行动可能导致供应链上传输的产品和服务的破坏。由于互联网技术的发展和普及,攻击者可以利用的执行攻击的途径数量众多,供应链的所有方面都可能遭受网络攻击

或者操控，包括设计、制造、传输和运送、安装、维护或者升级。ICT 供应链面临的威胁的很大部分由网络造成[CU2010]。

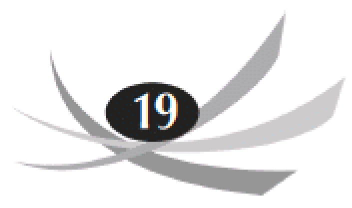
很多网络威胁由网络攻击造成，例如：拒绝服务攻击使网络被淹没于非法流量中，最终导致不能对合法要求做出响应；病毒通常会用一些诱人的名字来引诱用户采取一些行动，可能是打开一个邮件的附件或者访问一个特别的网站；蠕虫以攻击一个软件的弱点开始(这个弱点可以让软件的安全策略被故意地违反)，一旦电脑被感染，蠕虫就会竭力找到并感染其他电脑并在没有用户干涉的情况下自行传播；特洛伊木马是宣称一件事情，而实际上背后做的却是另外一些不同的事情，通常它的程序中会包含另一个程序，而这个程序会被定时器或者某个事件激活；钓鱼攻击会使用户收到一封邮件，欺骗用户去登录一个貌似合法公司的页面并提交自己的私人信息，而这些认证信息可以用于身份盗用；间谍软件可以使用户在安装一些软件产品的时候不知情地被安装了其他软件，表面上，间谍软件的目的是监测用户的浏览习惯以更好地为他们提供广告服务，而实际上，它可以暗中破坏并收集如密码之类的个人信息；还有键盘日志、网络爬虫、组合攻击等各种各样的网络攻击，严重威胁着 ICT 供应链的正常运行。

如果攻击者希望制造一些事端的话，那首要的任务就是获取目标网络的更多信息，也就是让他们查明怎样去攻击和攻击什么。攻击者的兴趣是：正在运行什么操作系统——可能会有一些后门或者补丁会成为攻击点；正在运行什么应用系统——他们可能会呼叫其他服务器或者互联网，哪一个可以被攻击；网络看起来如何？什么和什么连接着？在某些时候，你可能会有一个保护得很好的昂贵的服务器正与某些相对不明的地方连接着。攻击者会在网络上发布一些数据用来观察网络如何反应。另外，当企业或者政府机构的员工回到家中(也许仍然在工作)，攻击者开始在那里安置一些东西。人们再把他们已经感染的笔记本(或者 USB 插口或驱动器)带到单位里，就会导致蠕虫和间谍软件对网络系统的感染。还有另一种情况是攻击者就是员工之一，或者其他一些可以访问网络的人。

总而言之，攻击的生命周期可以从侦察开始，在这里攻击者会竭力找到更多相关网络的信息。这个发现阶段可以包括发现主机——攻击者会尽力找到被攻击网络上的服务器；服务发掘——他们会尽量找到正在运行的协议或者服务；网络映射——他们会弄清楚连接的方式；指纹识别——他们会观察你在运行何种操作系统等类似信息。攻击的生命周期也可能在侦察之后或者自行产生。这个阶段包括不知名的攻击或者瞬时攻击(zero-day attack)(这些攻击产生时没有任何迹象)，已知的攻击和它们的变种(可能有迹象)和阻断服务攻击。

最后，一旦攻击成功攻入网络，它将尽力地像蠕虫一样复制自己，也会竭力与源头联系，发送收集到的信息。整个攻击发生的阶段一般分为：侦查阶段、攻击阶段、繁殖/增殖阶段。侦查阶段是指攻击者扫描或者探寻服务器；攻击阶段则说的是一旦服务器的漏洞被发现，攻击程序便会启动，获取服务器的网络管理员权限；繁殖/增殖阶段表明在获得管理员密码后，利用与后台的“信任关系”征服新的服务器，或者当后台服务器的管理员密码被获取，攻击者就会建立一个到被攻击者的网络隧道，从而控制目标网络。

全世界范围内供应链的用户缺乏必要的硬件或者软件安全技术和业务程序，不能获得较好的安全环境。全球供应链对技术的依赖程度越来越高，面对网络威胁的脆弱性也



在增长。反过来,不断扩大的供应链连通性也使现有的网络安全威胁严重化。发展有效的全方位的网络安全战略,应对这些威胁已经迫在眉睫[CU2010]。

2.4.2 网络威胁的动因

在匿名化的网络空间中,人们可以共同制订计划并协调实施行动。攻击者在攻击之前、攻击过程中或者攻击之后可能都从未谋面。攻击可能对个人、公司、政府造成威胁。为了标定某个具体的系统,攻击者一般来说必须要做到以下两件事情中的一件:发现弱点,建立立足点,获得进入系统运算资源的特权,或者使系统过载引起功能错乱。在网络能力如此强大的今天,无论是个人、犯罪团体、流氓国家和恐怖主义分子都可以很容易地联结在一起造成一定程度的网络威胁,他们可能出于以下原因实施网络攻击[CU2010]。

(1) 个人利益的驱使。网络威胁频谱最低层级是独立行事、没有协作的个人行为。尽管一些个人行为者拥有很高的行动水平,可以对系统造成威胁,但是他们的动机仅限于获得个人利益的满足,或者实现他们希望引起的破坏目的。通常情况下,个人可以使用的资源有限,这一级别的危险程度较低[CU2010]。

(2) 企业利益的驱使。作为最大化投资收益的一种手段,商业间谍在网络空间也获得了发展。不管出自于企业行为者,还是所有层级的网络行为者,商业间谍行动都破坏着公平交易原则,这样的行为常常受到国家的支持,一些国家将此作为以较低投入获得社会进步和工业基础发展的手段,这将严重破坏和扰乱市场秩序,给其他合法经营者带来巨大损失[CU2010]。

(3) 国家利益的驱使。对一个国家来说,信息系统作为政府治理手段的关键部分有着重要价值,但是有些国家可能会出于政治利益的考虑,利用信息系统来破坏其他国家的安全。在国家安全领域,计算机系统被用来破解加密信息、破坏通信和指挥控制系统的事件由来已久。在网络领域,身份是难于跟踪的,所以很难确定一次特定攻击背后的国家,网络的匿名性在某种程度上使这种威胁行为更加猖獗。在审视网络安全环境时,不难发现网络威胁已经危害到了许多国家的国家利益,公民的计算机已经在遭受恶意软件的感染,并不知不觉地被用来危害国家利益。政府也不时受到网络攻击。许多国家的关键基础设施正在成为敌对国朝思暮想利用和打击的目标[CU2010]。

例如,美国的国家利益就受到了 ICT 供应链中的网络威胁的严重打击。美国战略和国际研究中心的研究结果表明,美国 50%以上的商业运作基础设施,包括电网和石油天然气供应设施,已经经受过了网络攻击,单日损失达数百万美元以上,这对社会服务是一个巨大的威胁。尽管美国在现代化的、联通的、高带宽的网络世界里占有安全软件的优势,然而攻击国也在努力发展开发性技术,并从经验中学习,完全有能力在网络空间中对美国发起攻击性的行动。信息和通讯领域制造业产品的全球化意味着美国和其他发达国家,包括所有的 G20 成员国在内,都依赖这一领域新出现的技术生产者[CU2010]。

(4) 罪犯和犯罪企业非法利益的驱使。网络空间的许多威胁都是受个人经济获益驱动或者与故意破坏公共(他人)的犯罪行为相关的。网络空间内的罪犯和犯罪企业已经越来越组织化,形成了高度组织化的个人信息、信用卡、身份和其他有价值信息的流动环。许多时候,罪犯和犯罪企业软件和硬件的发展能力可匹敌于工业领导者发展的软件和硬



件能力[CU2010]。

(5) 恐怖主义实施活动的驱使。利用网络空间具有匿名性的特征,恐怖主义组织已经开始将国际互联网作为支持其招募人员、获取资金和实现组织目标的重要平台和手段。网络空间提供了一种资助恐怖主义活动的简易方式,可以通过匿名的在线交易系统传送资源。它还提供了传送信息、提供指挥控制的手段。由于恐怖主义活动和犯罪企业不一样,其活动动机不完全是贪婪,所以这种活动更难应对[CU2010]。

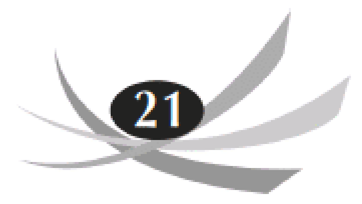
2.4.3 网络威胁的非对称性

20 世纪 90 年代,随着信息技术市场比重的增长和国际互联网的发展,人们将注意力投向了(网络)作为不对称战争的新形式。用来描述某个系统脆弱度的一个常用机制是描述那些暴露在威胁之下的“表面领域(surface area)”。由于大量的系统都联结了国际互联网,网络空间暴露出的是一个巨大的“表面区域”,存在可以利用的无数弱点。交汇的计算机和通信技术使得网路空间的“表面领域(surface area)”越来越大,导致了网络行为者的不对称性越来越突出。除了一台联结国际互联网的计算机外,网络攻击者对于优势技术和行动资源的需求是非常低的,他们进入和利用网络的成本也很低,从而使发起攻击的成本很低,而且失败或者被抓的几率比较小(根据现有的技术水平,将某次网络攻击或者操作同一台计算机联系起来是比较困难的。即使新技术可以更好地识别出一台具有攻击行为的计算机,但是由于僵尸网络和其他形式网络操作的存在,并不能确定计算机的所有者就一定参与了攻击行动)。一次网络攻击可以造成的破坏的量,要远远超出规划、发展和执行攻击所需的资源成本的量。尽管攻击受到较好防护的系统可能需要更多的投入,不对称性较弱,但网络攻击一般来说都是高度不对称的,攻击者的投入都能获得极高的回报[CU2010]。

防御者只有在任何地点、任何事件中都获得成功,才能成功维护网络的安全,然而攻击者只需要在任意地点任意事件中偶尔获得成功就可能会造成意想不到的收获。某次攻击可以从数以十亿计的点上发起,攻击者可以使用任何人任何地点都可以实现的一般性技术。从攻击者的角度看,攻击常常呈现少数对许多、成本低、利用资源少的特征。攻击的影响可以是即时而明显的,也可以是潜伏而微妙的,持续数年才能被发现[CU2010]。

网络攻击造成的破坏程度大小各异,可以是人事系统出现故障导致停工,也可以是关键基础设施遭到破坏而危及生命。无所不在的弱点为系统破坏者提供了巨大的机会。网络空间中绝大部分的脆弱点是个人工作站或者价值有限的其他系统,以及那些经常使用计算机的个人。然而,攻击者已经找到了利用这些低价值计算机的巧妙方式。攻击者将大量这样的计算机植入僵尸网络,从而造成系统过载。攻击者发展僵尸网络可能是大规模攻击的初步阶段[CU2010]。

例如,美国的国家安全能力依赖于强大的实力、远离威胁的工业基地、安全的内部交通线和占有压倒性优势的后勤保障力量。然而在今天,计算机和通信技术的普及已经使美国“偏远”区域融入了一个网络领域之中,其中任何要素都可以高速连接,美国供应链的“免疫力”已经被消解。世界范围内网络空间的出现,使美国的通信、指挥、控制和循环与外部的这些要素交织在一起,而不管交织对象是敌是友。由于独立的、一体化的网络攻击



和其他非对称手段的存在，美国现在每天要应对的是数以百计，甚至数以千计的攻击。这些攻击来自已知和未知的敌人，来自无数的进入点，可以来自独居的黑客，他们可能在网络内外，可能在美国边境内外，可能是有意的攻击，也可能是无意的冒犯。还有很多攻击则是全球范围的敌对国家的大规模的、协调的攻击。网络武器无处不在，交织的、网络化的信息技术和通讯系统与其他技术进步相结合，使个人和小团体出人意料地拥有了可以挑战美国这样的超级强国的手段[CU2010]。

从“震网”病毒攻击伊朗核设施，到“毒库”病毒大量收集工业控制系统情报，再到目前新发现的“火焰”病毒肆虐中东地区、窃取伊朗大量政府高级官员重要电脑数据……ICT供应链逐渐引发了网络安全威胁的全新阶段，使用网络武器发动的网络战争，可以实现不损失一兵一卒对另一个国家造成打击，这种军事对抗的新模式已在国际上普遍形成共识。使用网络武器攻击不同于传统网络攻击，它直接窥视国家基础设施、重要工业控制系统、重要信息系统和基础信息网络、有价值的商业机构和科研部门等，并有可能对国家基础设施和核心部门造成致命打击。“震网”和“火焰”引发的连锁性攻击，加重了国际社会对网络战的忧虑，也促进了各个国家对网络空间力量的建设。和传统战争不同，网络战可被轻易用来打击任何国家，因而有越来越多的国家尝试通过这种相对隐蔽、平缓的方式进行外交战略威慑，给予对方以“颜色”。全世界只要有网络空间存在的地方，网络攻击对政府、企业和个人威胁事件就在反复发生。

2.5 应对威胁

我国拥有庞大但是并不健全的ICT供应链，这些供应链中可能隐藏着很多脆弱点，这将威胁整个ICT供应链的正常运作和运作质量，进而影响到以ICT供应链为核心的其他所有供应链，这种影响可能会涉及每一个公民、企业甚至国家。

对国家安全的直接攻击会破坏和消解政府保护其民众安全的能力。攻击者会通过攻击关键的系统和政府功能来直接摧毁社会。这些攻击也可能阻止国家军队与战斗区域内单位通信的能力，或者影响通过特定的远程资产来指导战斗的能力。对国家的间接攻击是通过操控或者利用各类信息，来破坏公民、其他政府和非政府组织对该政府的信任，这样的攻击可能会破坏或者颠覆相关的例行规划。间接攻击还可能通过对不太重要的功能进行分散式的攻击来影响社会的士气。政府必须要确立有效的计划和程序来反制这两种类型的攻击，将ICT供应链面临的威胁降到最低[CU2010]。

企业不仅拥有和操作着一些关键基础设施，还管理和运行着绝大多数的ICT供应链，支持着其他供应链。因此，企业ICT供应链面临的威胁将最大范围地影响到整个社会。企业必须正视这种威胁，意识到它会严重危害企业的利益，甚至带来灭顶之灾，因而必须采取相应的应对措施来预防这种威胁[CU2010]。

每一位使用个人计算机、智能电话或者其他可以联结到国际互联网的装置的人，都是一位潜在的网络战斗者。每个人都有责任和义务来确保他们和其他人使用的系统的安全，无论是从个人角度出发，还是从公共角度出发，无论这个人是某个机构的雇员，教育机构的学生还是任何其他的社会角色。采取积极的措施应对ICT供应链威胁，无论对国

家、企业还是个人，都是刻不容缓的事情[CU2010]。

参 考 文 献

[BAH2012] Booz，Allen，Hamilton. Managing Risk in Global ICT Supply Chains-Best Practices and Standards for Acquiring ICT. 2012.

[CU2010] CACI，USNI. Cyber Threats to National Security，Symposium One：Countering Challenges to the Global Supply Chain. 2010.

[DXT2009] 董绍辉，西宝，田丽娜. 供应链信息泄露途径及其防范措施. 商业研究，2009.

[GPL2011] 郭茜，蒲云，李延来. 供应链中断风险管理研究综述. 中国流通经济. 2011.

[HCL2004] Hays C L. What Wal-Mart Knows About Customers' Habits[N]. The NewYork Times. 2004.

[MT2007] Murphy T. Protection In Question[EB/OL]. 2007.

[NYM2011] 倪媛明. 供应链风险的形成与控制研究. 中国市场. 2011.

[USGAO2012] United States Government Accountability Office. IT SUPPLY Chain National Security-Related Agencies Need to Better Address Risks. 2012.

[WH2010] The White House. US National Security Strategy. May 2010.

[YZG2011] 阎子刚. 供应链管理. 2 版. 北京：机械工业出版社. 2011.

[ZX2012] 钟玉洁，薛云建. 基于弹性供应链的供应中断风险应对. 中国物流与采购. 2012.

[WZ1] http://info.1688.com/detail/1019802467.html? u=.

[WZ2] http://cn.made-in-china.com/info/article-2104594.html.

[WZ3] http://jjckb.xinhuanet.com/opinion/2011-10/27/content_339501.htm.

[WZ4] http://www.1mfg.com/1mfg/j/StoryAff/show/31575.shtml.

第 3 章

国外 ICT 供应链安全战略

3.1 概　　述

ICT 供应链的独特性给世界各国带来了很多新的安全挑战,针对目标的供应链攻击成为攻击其 ICT 系统的一条重要路径。因此,确保 ICT 供应链的安全,已经成为增强国家信息安全保障的一项基础性工作。面对日益复杂的供应链,世界各国,尤其是技术发达、网络依赖程度较高的国家,已逐步开始将 ICT 供应链安全列入其国家战略,并付诸了实践。

当前,ICT 供应链安全研究主要集中在美国和欧洲。美国掌握着世界上最先进的信息通信技术,其 ICT 企业在全球市场占据垄断和主导地位。但美国仍将 ICT 产品的供应链安全作为加强其自身信息安全保护的重要考虑。从克林顿政府时期的"关键基础设施保护"、"深度防御",到布什政府的"保护网络空间的国家战略"、CNCI 计划等,再到奥巴马政府"联邦信息系统供应链安全风险管理指南",美国政府对 ICT 供应链的重视程度逐年增加。

欧盟作为世界第一大经济体,欧盟的信息化水平一直居前茅,一个最经典的例子就是欧盟各成员国的基础设施已经做到了相互连通。然而,欧盟在制订整体信息安全政策方面一直步履蹒跚。尽管如此,欧盟近年来在信息通信供应链安全相关方面还是取得了一些进展,紧随美国之后,对 ICT 供应链安全也愈发重视,并发布了一些相关战略,如发布《关键信息基础设施保护》、加强与美国的合作、成立"欧洲网络与信息安全局"等。

其他一些 ICT 技术较发达的国家,如英国、德国、法国、俄罗斯和澳大利亚等国,面对国内和国际上的 ICT 和网络空间安全威胁和挑战,也相继提出了一些与 ICT 供应链相关的国家战略和政策,并正在逐步付诸实践。虽然这些国家没有像美国一样明确地定义其 ICT 供应链战略,但从其国家安全战略,尤其是网络安全战略中,也可窥探出一二。因此,本书对于其他国家和地区 ICT 供应链战略的介绍主要集中在网络空间安全层面。例如,英国曾于 2009 年和 2011 年先后提出了两个涵盖 ICT 安全的网络信息安全战略;德国也在大力发展 ICT 技术的同时,明确了网络安全战略;法国根据其 2008 年发布国防白皮书要求于 2009 年成立了网络与信息安全局,其职能便包括为政府和企业提供可信的产品与服务等关于 ICT 供应链安全的重要内容;俄罗斯在发展其 ICT 战略的同时也十分重视信息基础设施的保护;澳大利亚政府十分重视国家 ICT 基础设施的保护、网络身份和隐私的保护以及灾难恢复能力的建设,建设有严密的安全系统和防范措施,注重调动全社会的积极参与、注重信息安全测评体系建设、注重国际安全合作。

3.2 美国ICT供应链安全战略

3.2.1 美国安全战略的发展

美国最早对ICT供应链安全的关注始于克林顿政府，当然，当时还没有正式提出ICT供应链的概念，但其战略实质却与之息息相关。由于ICT供应链面临的首要威胁就是来自网络空间的威胁，因此，国家的信息安全战略也成为了ICT供应链安全战略中的重要一环。

1. 克林顿时期

1993年，克林顿政府提出兴建“国家信息基础设施”。1998年5月，克林顿签发《关键基础设施保护》总统令[PDD-63]，首次明确信息网络安全战略的概念、意义和长期短期目标。该命令开宗明义地说明，世界上最强大的军事力量和经济力量相互促进和依赖，但是也越来越依赖某些关键设施和以网络为基础的信息系统。所谓关键基础设施是“指那些对国家十分重要的物理性的以及基于计算机的系统和资产，它们一旦受损或遭破坏，将会对国家安全、国家经济安全和国家公众健康及保健产生破坏性的冲击”。关键基础设施日益自动化、相互联结，但是这种先进性却对网络袭击越来越脆弱。美国应该从国家战略高度保护包括网络在内的基础设施。该命令并对今后一段时间内，加强基础设施安全作出了指示，即对脆弱性进行评估；制订补救计划；进行预警；实时反应；对破坏的关键基础设施进行重建；教育民众，让其知晓关键基础设施的重要性；研发相关技术；加强情报工作；进行国际合作；采取立法与预算措施。

1998年年底，美国国家安全局(NSA)公布《信息保障技术框架》(IATF1.0)，提出“深度防御战略”(Defense-in-Depth)。所谓深度防御战略就是采用一个多层次的、纵深的安全措施来保障用户信息及信息系统的安全。在深度防御战略中，人、技术和操作是三个主要核心因素，是保障信息及信息系统的安全的关键。IATF将信息系统的信息保障技术层面划分成了四个技术框架焦点：网络和基础设施、区域边界、计算环境和支撑性基础设施。

2000年1月，克林顿政府发布了《信息系统保护国家计划》(NIPP1.0)，强调国家信息基础设施保护的概念，并列出了可能对美国网络关键基础设施发起攻击的六大敌人：主权国家、经济竞争者、各种犯罪、黑客、恐怖主义和内部人员。

克林顿时代的《信息系统保护国家计划》率先提出重要网络信息安全关系到国家战略安全，把重要网络信息安全放在优先发展的位置，并对重点信息网络实行全寿命安全周期管理。按照要求，新建和正在运行的重要信息网络的信息系统必须实施定期风险评估，针对信息系统的安全类别和等级，实行等级保护，并定期通过安全测试和风险评估，由联邦机构的高级官员基于安全控制的有效性和残余风险值决定是否授权该信息系统投入运行。这些风险评估的方法，逐渐成为全球信息系统安全评估的模式。可以看出，克林顿时代的网络安全战略重点在于“全面防御”。

2000年12月克林顿总统签署《全球时代的国家安全战略》[GNSS2000]文件，是美国

国家信息网络安全政策的重大事件。文件将信息网络安全列入国家安全战略，成为国家安全战略的重要组成部分。这标志着网络安全正式进入国家安全战略框架，并具有独立地位。

克林顿时代从保护关键基础设施来确保网络安全，其中一个关键问题就是防范恐怖分子利用网络对美国发起恐怖袭击，采取一切必要措施，迅速消除导致关键基础设施面临物理和网络攻击的明显弱点。虽然没有明确提出ICT供应链的概念，但保护信息关键基础设施的实质是保护ICT供应链安全的重要环节[CQ2010]。

2. 布什政府时期

《国家信息系统保护计划》设想到2003年5月完成对信息系统的保护。但是不幸的是，克林顿政府所担心的事情在2001年9月11日发生了。“9·11事件”加速了美国政府对关键基础设施的保护，强化了美国对网络安全战略的实行。

“9·11”事件以后，出于反恐的需要，这方面的措施还得到了进一步的加强。2001年10月16日，布什政府意识到了“9.11”之后信息安全的严峻性，发布了第13231号行政令《信息时代的关键基础设施保护》[CIPIA2001]，宣布成立“总统关键基础设施保护委员会”，简称PCIPB，代表政府全面负责国家的信息安全工作。该委员会成员包括国务卿、国防部长、司法部长、商务部长、国家经济委员会主席、总统国家安全事务助理等官员。根据该命令，委员会主席将成为总统网络安全事务顾问。他有权了解各部门内属于其管辖范围的所有情况，并召集和主持委员会的各种会议、制定委员会的议事日程，向相关官员提供保护关键基础设施的政策和方案，并向总统国家安全事务助理汇报。PCIPB成立后，为布什政府从两个方面着手确保网络安全。一是，制定关键基础设施的保护；二是，制定网络安全战略，两个方面互相促进。

2002年3月20日向美国民众公布了国家战略中可能会涉及到的53个重点问题，广泛听取国民的意见和建议。在这53个问题中，已经开始正式关注供应链，要求研究供应链与信息安全风险的关系。但是，该阶段的美国信息安全战略主要是从国内大型企业运行安全的角度看待供应链问题，更多的是强调企业要加强与供应链的互动。

在整理国民对53个问题的反馈意见基础上，2003年2月14日发布了《保护网络空间的国家战略》[NSSC2003]，共76页。该报告确定了在网络安全方面的三项总体战略目标和五项具体的优先目标。其中的三项总体战略目标是：阻止针对美国至关重要的基础设施的网络攻击；减少美国对网络攻击的脆弱性；在确实发生网络攻击时，使损害程度最小化、恢复时间最短化。五项优先目标是：

(1) 建立国家网络安全反应系统；

(2) 建立一项减少网络安全威胁和脆弱性的国家项目；

(3) 建立一项网络安全预警和培训的国家项目；

(4) 确保政府各部门的网络安全；

(5) 国家安全与国际网络安全合作。

该报告明确规定，国土安全部将成为联邦政府确保网络安全的核心部门，并且在确保网络安全方面充当联邦政府与各州、地方政府和非政府组织，即公共部门、私营部门和研究机构之间的指挥中枢。国土安全部将制订一项确保美国关键资源和至关重要的基础设

施安全的全面的国家计划，以便向私营部门和其他政府机构提供危机管理、预警信息和建议、技术援助、资金支持等5项责任。该报告把关键基础设施定义为“那些维持经济和政府最低限度的运作所需要的物理和网络系统，包括信息和通信系统、能源部门、银行与金融、交通运输、水利系统、应急服务部门、公共安全以及保证联邦、州和地方政府连续运作的领导机构”。该报告强调，确保美国网络安全的关键在于美国公共与私营部门的共同参与，以便有效地完成网络预警、培训、技术改进、脆弱性补救等工作。

2003年2月14日同时签发的《关键基础设施和重要资产物理保护的国家战略》[NSPP2003]作为《保护网络空间的国家战略》补充部分。关键基础设施，是系统和资产，不管是物理的、还是虚拟的都对国家至关重要，他们能力不足或者毁损对国家安全、国家经济安全和国民健康，都会产生影响。国家战略是美国政府制订保护关键基础设施计划的基础。布什任内国土安全部先后两次颁布《国家基础设施保护计划》（National Infrastructure Protection Plan，NIPP），具体地说明了如何保护这些关键基础设施和重要资产。在这个文件中，布什政府重新界定了关键基础设施，取代克林顿政府时期的界定。布什政府改变克林顿政府没有说明、区分关键基础设施和主要资产的做法，把通信、信息技术、国防工业基础等18个基础设施部门列为关键基础设施，并把核电厂、政府设施等5项列为重要资产。

在布什政府执政后期，随着全球信息安全形势日益严峻，ICT供应链安全问题开始进入政府的视野。

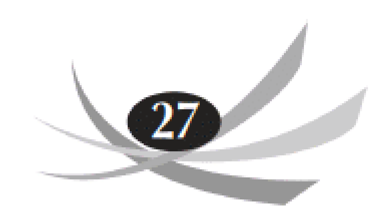
2006年4月，美国国家科技委员会发布了《联邦网络安全和信息保障研发计划》[FPCIRD2006]，明确将ICT硬件和软件的供应链攻击列为一种攻击趋势，并认为这种安全问题仅靠严格检测是无法解决的。但是，这个计划中仅将供应链攻击视为一种特殊的“内部人员攻击”。

美国国土安全部在2007年专门发布了《增强国际供应链安全的国家策略》[SEISCS2007]。

2008年1月，布什发布了54号国家安全总统令（NSPD54），同时也是第23号国土安全总统令（HSPD23），提出了国家网络安全综合计划（Comprehensive National Cybersecurity Initiative，CNCI）。该计划中的第11项任务就是建立全方位的方法来实施全球供应链风险管理。该计划提出：

“商用信息通信技术市场已经全球化，这为那些试图通过渗透进供应链来非授权访问数据、篡改数据或拦截通信信息，从而危害美国的人们提供了更多的机会。必须采用能够涵盖产品、系统和服务的完整生命周期的战略性、综合性方案，对来自国内和全球供应链的风险加以管理。这种风险管理要求对威胁、漏洞以及采办决定的后果具备更强的意识，要求开发和部署能在产品生命周期内（从设计到报废）从技术和操作层面减少风险的工具和资源，要求建立能够适应复杂的全球化市场的新采办政策和实践措施，要求与工业界合作制定和采用供应链与风险管理标准及最佳实践措施。该项活动将使联邦政府向各部门提供强健的供应链风险管理与控制工具集的能力、政策和流程得到强化，使经过管理和控制后的供应链风险同系统与网络的重要性相称。”

这说明，美国已经将ICT供应链安全问题上升到了国家威胁及对抗的层面，标志着



美国对ICT供应链安全的认识达到了全新的高度。

3. 奥巴马政府时期

2008年12月，在奥巴马上台之前，美国智库战略与国际研究中心(CSIS)发布了《在第44任总统任期内保护网络空间安全》的咨询报告[SCP2008]，向新总统提出了若干重要建议。其中便包括“通过采购规则提高安全性”，希望政府能与工业界合作，共同制订和执行ICT产品(其中软件居首要位置)采购安全指南。

奥巴马政府执政后，进一步重视信息安全问题，将信息安全视为最严重的经济和国家安全挑战之一。2009年5月，奥巴马政府发布了对美国网络空间安全政策的评估报告[CPR2009]，并根据评估结果开展了新一轮的动作。这个评估报告继承了国家网络安全综合计划(CNCI)对ICT供应链问题的判断，将其作为国家信息安全威胁的一种，重申了采取综合、体系化对策的重要性。从其措辞不难发现，美国已经完全将ICT供应链安全问题与“国外”机构相提并论。奥巴马政府在报告中同时提出，仅仅谴责国外产品和服务供应商是不够的，新的供应链风险管理方法势在必行。

美国国土安全部国家网络安全处软件保障主管乔·哲伯克在2009年召开的Web应用安全计划会议上的观点代表了美国政府对ICT供应链安全问题的战略定位：“软件供应链风险管理是一个国家安全问题”，硬件同样包括在内。

2010年6月，美国NIST发布《联邦信息系统供应链安全风险管理指南》[PSCRM2010]，成为美国在解决ICT供应链安全方面指导手册的试行版。与此同时，美国还在立法上采取一系列措施，配合供应链安全风险管理的实施。

2011年5月，美国发布《网络空间国际战略》[ISC2011]，在该报告的第三部分，优先政策中，在论述保护网络空间安全，加强安全性、可靠性和灵活性时，指出：

“**经与工业部门磋商，加强高科技供应链的安全性**。关键网络和信息基础设施的顺利运行在于能否保证有可靠的软硬件。供应链中的漏洞能破坏网络和网络所包含数据的完整性、可用性和保密性。这些漏洞一旦被利用就会削弱经济能力损害国家安全。美国将与工业部门、国际合作伙伴合作找出保护信息系统和关键基础设施完整性的最佳方法。这样，我们将大大提高基于自由开放贸易的全球化供应链的安全性。”

2012年1月25日，在瑞士举行的达沃斯世界经济论坛上，美国国土安全部长Janet Napolitano对外公布了一个新的安全政策，即《全球供应链安全国家战略》[NSGSCS2012]。该战略有两个目的：首先，提高全球商品运输的效率与安全，其次，为全球商品运输提供一个更加有弹性的供应链系统。至此，ICT供应链安全正式提升到了美国国家战略的层面。

奥巴马在为该战略所做的序言中提出，全球供应链系统对美国的经济和安全至关重要，是一项关键的全球资产，为应对各种针对供应链的威胁，必须通过《全球供应链安全国家战略》使之得到加强，从而保障经济的繁荣。这一战略是“一项举国上下的方略，以及国际社会之间的积极协作。”奥巴马说“我们将建立层次分明的防御力量，及早地应对威胁，培育一个能够承受意想不到的破坏并从中迅速恢复、具有韧性的系统，以增强应对风险的能力”。

这一战略具有深远意义。它不仅将应用于通过船舶、飞机或卡车进入美国的所有货

物，还可能为美国采取行动、帮助其他国家加强安全打下基础。该战略的推出给我们的启示是多方面的，美国最高领导人亲自作序，并联合各方共同推进这一举国上下的战略，目标明确，措施具体，值得他国学习和借鉴。

2013年8月，NIST又发布了《联邦信息系统和组织供应链风险管理方法》草案[NIST SP 800-161]，旨在指导联邦部门和机构在组织层面上识别、评估和减轻ICT供应链风险。

3.2.2 美国的政策与立法保障

在不断强化ICT供应链安全战略重要性的同时，美国也先后在政策法规中提出了多项要求。

1. 国家安全系统领域对ICT产品的采购要求

美国的国家安全系统是指对于国家安全至关重要的信息系统，2003年8月发布的《将信息系统标识为国家安全系统的指南》[NIST SP 800-59]对如何确定国家安全系统提出了明确规定。早在2001年，美国国家安全电信和信息系统安全委员会(National Security Telecommunications and Information Systems Security Committee，NSTISSC)便宣布，自2002年7月起，在国家安全系统中强制使用经过美国国家信息保障联盟(National Information Assurance Partnership，NIAP)认证的ICT产品。虽然美国已与其余20多个国家共同签署了信息技术安全通用评估准则(CC)的互认协定，但其国家安全系统的采购清单上迄今没有出现过由他国信息安全认证机构认证的信息技术产品，这使得以华为、中兴、联想为代表的中国企业在美国市场屡屡碰壁。

2. 在联邦信息系统安全指南中提出的安全控制要求

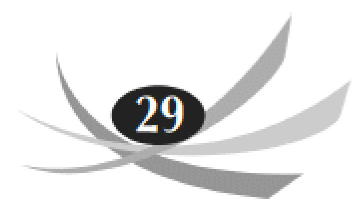
美国国家标准与技术研究院(NIST)在发布《对联邦信息系统和组织的安全控制建议》[NIST SP 800-53]时，将“系统和服务采购”列为一项重要的信息安全控制类。该控制类中的第12项要求便是“供应链保护”，其安全控制措施要求联邦政府机构对供应链安全风险进行防范，在系统全生命周期范围内关注脆弱性。可选的增强性措施包括：在采购系统软硬件和服务前就要对服务提供商进行细致审查和选择，建立可信的交付渠道，在同一系统中要采购多个供应商的产品，缩短采购决定和交货的时间差，必要时对系统进行渗透性测试。根据《联邦信息安全管理法案》，NIST发布的SP 800-53对所有的联邦机构都具有强制性作用。

3. 立法中对联邦政府采购制度的改革要求

2010年3月，美国参议院通过了《网络安全法案》[CA2009]。这是美国历史上一部很少见的综合性的信息安全法案。它高度关注联邦政府的ICT供应链安全，为联邦政府采购ICT产品提出了法律条款。根据该法案的规定，采购工作的责任部门是总务管理局，实施途径是由总务管理局制定统一的信息要求书(RFI)和建议要求书(RFP)格式，在其中明确对ICT产品和服务的安全要求，任何联邦机构不得违背。

4. 立法中提出的研发要求

奥巴马政府在网络安全政策评估中提出，要充分发挥技术创新对解决供应链安全问题的重要作用，且要通过技术创新确保美国企业的市场领先优势，其实质是消除美国对国



外产品和服务的依赖，并控制全球ICT市场的发展。因此，近年来美国连续出台多个法案或提出法律议案，对创新性的ICT技术和信息安全技术予以高额资助。此外，美国还高度关注通过技术手段来化解供应链安全风险。前面谈到的《网络安全法案》要求支持以下技术的研发：测试和验证来自国内或第三方软件中的重大已知安全缺陷，测试和验证第三方软件的功能是否正确以及是否嵌入了其他功能[ZXD2010]。

5. 对加强ICT供应链安全管理做出的工作部署

事实上，美国近年来所开展的一系列加强供应链安全管理的活动都来自于第54号国家安全总统令对国家网络安全综合计划（CNCI）的部署。在提出要研究战略性、综合性的供应链风险管理方案时，该总统令重点如下：

- 要对威胁、漏洞以及采购决定的后果具备更强的意识；
- 要开发和部署能在产品生命周期内（从设计到报废）从技术和操作层面减少风险的工具和资源；
- 要建立能够适应复杂的全球化市场的新型采购政策和实践措施；
- 要与工业界合作制订和采用供应链与风险管理标准及最佳实践措施。

3.2.3　美国供应链安全实践

1. 美国政府的活动

为落实54号国家安全总统令对ICT供应链安全问题的部署，美国联邦政府和军方成立了专门的组织，如图3-1所示。目前，已经有4个工作组开始运转：高级指导组、采购政策和法律分析组、生命周期过程和标准工作组、威胁信息共享工作组。其中，高级指导组起组织协调作用，具体由国土安全部（DHS）和国防部（DOD）负责；采购政策和法律分析工作组旨在通过政策和法律层面评估是否可以利用情报部门提供供应链安全风险信息，以及利用非情报部门（包括销售商）提供重要信息，具体由管理和预算办公室（OMB）以及总务管理局（GSA）负责；生命周期过程和标准工作组旨在制定供应链安全风险管理

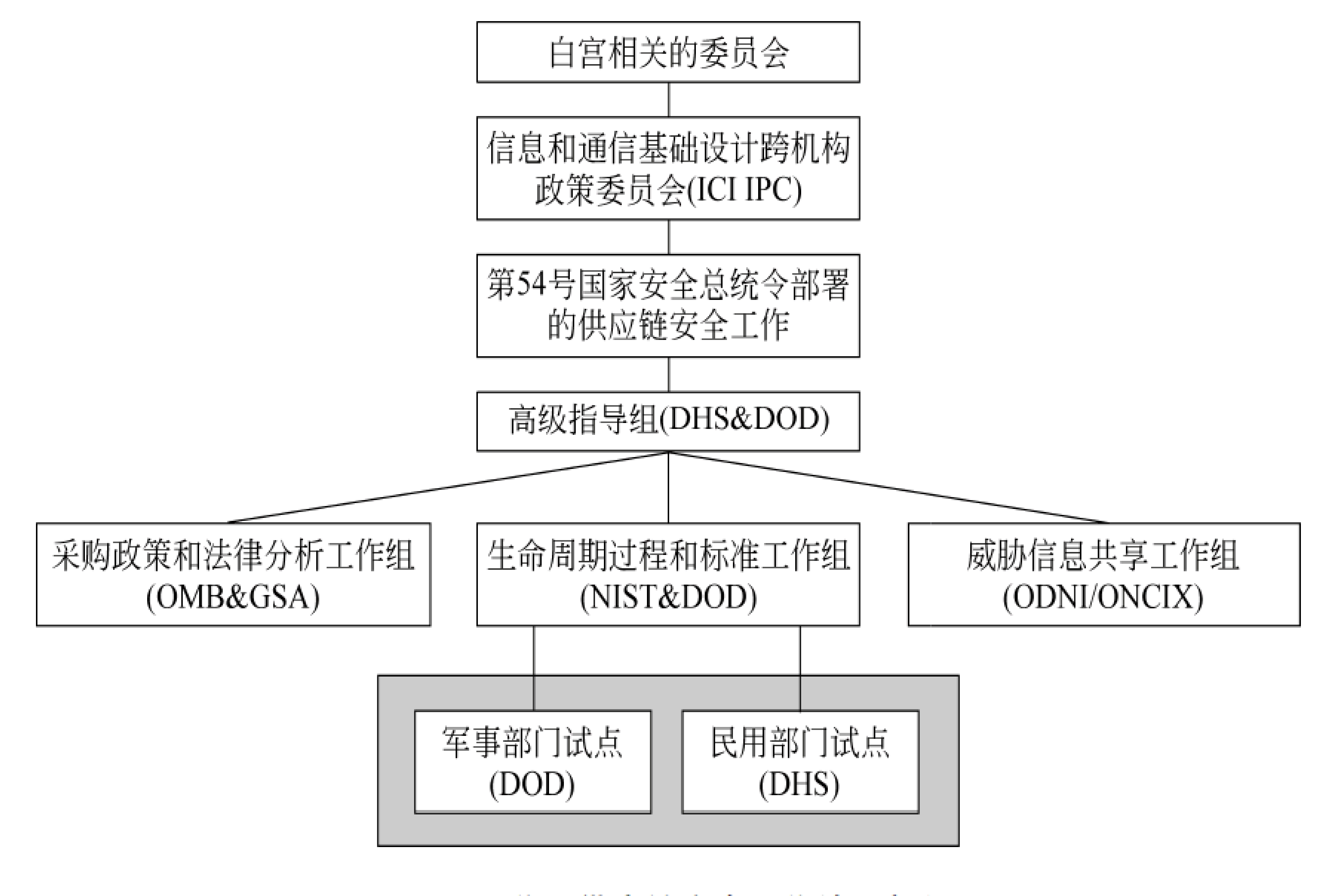


图3-1　美国供应链安全工作涉及部门

标准和有关指导性文件，具体由NIST和国防部(DOD)负责；威胁信息共享工作组负责在整个联邦范围内共享供应商威胁分析信息，具体由国家情报部总监办公室(ODNI/ONCIX)负责。

目前，工作组中的很多活动都已开展。例如，在生命周期过程和标准工作组，NIST提出了“广度防御”的战略，是对美国国家安全局在《信息保障技术框架》中提出的“纵深防御(Defense-in-Depth)”战略思想的发展。NIST认为，纵深防御战略侧重于通过分层的防御体系对网络和系统进行保护，其关注的是产品在运行中的安全，因而完全不能解决供应链安全问题。而广度防御战略的核心是在系统的完整生命周期内减少风险。相信这一思想的提出将对美国的信息安全活动产生重要的影响。

美国各机构在供应链安全方面的具体工作：

- 美国国防部(DOD)：成立了供应链风险管理计划，从系统确保层面增强供应链安全。
- 美国国家安全局(NSA)：成立了供应链风险管理特别计划办公室、软件确保中心、恶意代码老虎队及反伪造小组等，确保供应链安全。
- 美国国土安全部(DHS)：成立了软件确保计划，以及漏洞挖掘和修复计划。
- 美国国家标准研究院(NIST)：研究制定供应链风险管理规范，承担软件确保机制和工具评估项目的研究。

2. 学术界和企业界的主要活动

对于政府的ICT供应链安全管理战略，学术界和企业界有非常积极的响应。目前，美国已经成立了多个专门研究ICT供应链安全的学术组织，一些企业也推出了ICT供应链安全管理工具，ICT供应链安全研究进入了一个非常活跃的阶段。

2009年，受政府资助的美国信息基础设施安全保障学会向参议院提交了《国家网络安全研究和开发挑战》的报告[NCSR2009]。这份报告明确提出，来自于海外的硬件和软件正在面临被恶意修改的危险，威胁已经迫在眉睫。其甚至对包括ICT供应链威胁在内的若干典型威胁作了如下后果描述：计算机只要上网就会受到攻击。同年6月，美国科学应用国际合作组织(SAIC)和马里兰大学史密斯商学院供应链管理中心联合发布了合作完成的题为《建立网络供应链保障参考模型》的研究报告[BCSCRM2009]，强调在网络供应链生命周期中进行安全保障。研究人员在全球供应链发展的最佳实践经验基础上，首次提出了一个供应链安全保障模型。该模型对ICT软件和硬件的特征做了充分考虑，从用户层、控制管理层、供应商层三个层面具体描述了保障供应链安全的具体措施。模型很好地体现了供应链安全风险管理和信息安全这两门学科的融合，不但对关键行动者、关键过程和薄弱环节进行了定义，还指出了国际生产和维护链条中每个节点的战略性依存要素。这一部研究报告在某种程度上代表了美国当前在ICT供应链安全风险管理研究方面的最先进成果，其研究结论已经对政府部门的活动产生了积极影响。例如，NIST正是从这一研究报告中提炼并发展了“广度防御”战略。

2010年3月2日，美国海军学会和CACI国际发起了题为“对国家安全的网络威胁：应对全球供应链面临的挑战”的学术研讨会。在这次研讨会上，专家各抒己见，形成了应对全球供应链挑战报告[CTNS2010]。这份报告主要阐述美国在网络时代面临的威胁以



及美国政府及社会对这种威胁的认知程度，细致分析了网络威胁对政府、私营部门、个人以及跨国公司的影响，分析了美国过去十分安全的全球供应链如今在网络威胁面前的脆弱性。报告认为，应对网络安全威胁对美国来说是一个庞大的系统工程，首先要通过研究确立网络安全领域的概念和术语；然后通过教育和战略沟通加深美国民众对网络安全威胁的认知；要通过有效立法，规范应对网络安全威胁的举措；要通过有力的行政作为，确保应对网络安全威胁措施的落实。报告最后还提出了切实的建议。

2010年5月，卡内基梅隆大学(CMU)软件工程研究所发布了《评估和降低软件供应链安全风险》的报告[EMSSC2010]，指出软件供应链安全风险管理必须贯穿整个采办周期，同时详述了那些能证明这些风险已经被适当减轻的证据必须被收集。供应链风险被降低的证明应该在采办周期的各个阶段都被收集：立项、开发、配置、部署、操作、维护、废弃。所需的证明包括：供应商生产安全软件能力的分析，交付产品的安全分析，在供应链的各个阶段保证产品严格实行访问控制的评估，在产品的使用年限里保证产品被正确的配置规程的分析。报告提供了一个“确保案例”参考模型，说明了这些被收集的证明如何结合在一个论据中证明在整个采办周期中，供应链安全风险已经被充分的认识和处理了。参考模型强调了两个主要的控制安全风险的策略：

(1) 识别和监视系统的表面攻击，

(2) 开发和维护一个攻击模型。这些策略的实施需要在采办周期的各个不同的阶段采取不同的行为。

2010年6月，美国SAFECode公司发布了《软件完整性控制——基于保障性的软件供应链风险最小化方法》报告[SIC2010]，阐述了软件生命周期中实现软件保障性的三个基本指标，即安全性、完整性和可靠性，并重点对软件完整性控制的相关措施和手段进行了介绍。报告指出：在软件、组件及服务的外包、开发、测试和分发的过程中，对软件供应链的各个环节实施完整性控制，是目前较为有效的工程方法。报告最后得出结论：进一步的深入研究以及工程化合作，将有利于该领域对软件完整性做出更突出的贡献。

2010年8月，美国国防部信息保障分析中心(Information Assurance Technology Analysis Center，IATAC)发布信息通信供应链风险管理报告[RMICT2010]，讨论了信息通信供应链本身以及软硬件所面临的威胁，指出了降低供应链风险的措施。该报告系统地调研了政界、企业界和学术界在解决供应链安全风险方面所做的努力。同年，在IATAC发行的刊物上撰文对该报告主要内容做了简介[SICTSC2010]。

2010年3月召开的第12届软件确保论坛对ICT供应链安全进行了详细探讨。在同年12月召开的第26届计算机安全应用年会(ACSAC)上，特别设立了供应链安全专题。来自美国NIST的Nadya Bartol、美国国防部的Don Davidson、美国国家安全局的Larry Wagoner、CMU软件工程研究所的Carol Woody以及SAFECode公司的Dan Reddy等人汇聚一堂，共同讨论供应链安全问题。而来自CVI分析公司的Frank E. McFadden在2010年的IEEE国土安全技术国际会议上对电子供应链风险降低技术进行了深入探讨。

2010年5月3日到5日，由著名智库东西方研究所(EastWest Institute)主办的首届全球网络安全峰会(Worldwide Cybersecurity Summit)在美国达拉斯召开。峰会演讲人员包括美国网络安全协调官Howard Schmidt，美国总统网络安全顾问James L. Jones，

欧洲网络与信息安全局负责人 Udo Helmbrecht，会计师事务所德勤公司首席执行官 James H. Quigley，华为首席技术官 Matt Bross，微软可信计算副总裁 Scott Charney 等政府官员、企业领袖和安全专家。在此次大会上，与会人员广泛探讨了有关公众信息安全意识普及，国家间信息安全协调合作，打击网络犯罪，加强政府与私营信息安全企业合作，信息与通信技术，互联网媒体，ICT 供应链安全等多个议题。东西方研究所同时提出了其全球网络安全计划，期望促成关键国家包括中国、美国、印度等建立有关网络威胁的共识。

2011 年 3 月 1 日在美国华盛顿州卡内基科学研究所举行了第五次"非对称威胁"讨论会，聚焦网络空间安全带给全工业基准(Industrial Base)的挑战，会后在 2011 年 9 月发布了《保障国家工业基准安全》报告[CTNS2011]。报告认为供应链为网络入侵提供了很多机会，尤其是随着无线技术的发展，访问变得更加容易。消除供应链中的入侵是一个很迫切的问题。

2011 年 3 月美国航空工业协会发布了《增强意识，抵制伪造》的报告[CIADC2011]，对美国航空工业供应链中的伪造产品进行了调研，提出了安全保障措施。

2012 年年初，世界经济论坛发布《解决供应链和运输风险的新模型》报告[EFNMASC2012]，对包括 ICT 供应链在内的供应链安全风险进行了阐述。这个供应链和运输风险报告回顾了外部冲击，网络趋势和漏洞，并提出了相应的对策建议。在本书第 4 章 4.6 节将对此进行详细介绍。

3.3 欧盟 ICT 供应链安全战略

3.3.1 欧盟 ICT 供应链安全发展

作为世界第一大经济体，欧盟的信息化水平一直居前茅，欧盟各成员国的基础设施已经做到了相互连通。然而，欧盟在制定整体信息安全政策方面一直步履蹒跚。尽管如此，欧盟近年来在 ICT 供应链安全相关的战略方面还是取得了一些进展，主要体现在以下方面。

(1) 欧盟委员会开始从战略高度关注信息基础设施安全。2009 年 3 月日在欧盟总部布鲁塞尔颁布了《关键信息基础设施保护》[MEMO-09-141]，2010 年 8 月 26 日颁布了《数字欧洲计划》等文件。

(2) 欧盟加强了与美国的合作。2010 年，美国总统奥巴马与欧盟主席巴罗佐在葡萄牙首都里斯本宣布成立美国—欧盟之间的网络安全联合工作组，其内容包括北约(The North Atlantic Treaty Organization，NATO)在危机处理、联合预警、防止儿童色情犯罪，以及指导欧盟在打击网络犯罪等领域方面加强合作。

(3) 成立了"欧洲网络与信息安全局"(European Network and Information Security Agency，ENISA)。该部门专门负责组织、协调欧盟各成员国的信息安全战略规划、实践、基础设施保护和应急响应等工作。

(4) 促成了世界上首部关于打击网络犯罪活动的国际条约——《网络犯罪布达佩斯公约》[CETS185]。

2012年6月，数字欧洲(DIGITAL EUROPE)、美国信息技术理事会(Information Technology Industry Council，ITI)、日本电子与信息技术行业协会(JEITA)在布鲁塞尔共同发布了名为《政府网络安全推荐准则》的声明，提出了12条原则，敦促个欧洲政府在制定网络安全相关法规和政策时遵守。

2012年10月，欧盟委员会向欧盟理事会和欧盟议会提交了“云计算发展战略及三大关键行动”建议草案。旨在加速欧盟云计算服务建设，尽快将云计算技术研发成果转入应用，到2020年实现欧盟云计算技术腾飞。

此外，为应对新的网络安全挑战，欧盟委员会在2013年1月11日在荷兰海牙成立了欧洲网络犯罪中心保护欧洲民众和公司不受网络犯罪的危害。该网络中心的成立加强了欧盟各国在打击网络犯罪方面的合作，为ICT及其供应链网络安全方面提供保障。

3.3.2 欧盟ICT供应链安全战略分析

2005年，欧盟委员会提出了在信息通信和服务工作中要特别重视供应链中各利益攸关方对可信、可靠和保密的要求。为此，欧盟在2006年出台了“安全的信息社会战略”。然而，该战略在责任主体和具体实施方面存在诸多缺陷。

为了弥补上述各方面的不足，2009年欧盟颁布了《关键信息基础设施保护》[MEMO-09-141]文件，旨在落实欧盟委员会近来一系列有关信息网络安全保护的决议案。该文件由三大核心内容组成，第一部分是现状分析：包括关键信息基础设施对欧盟社会经济生活的重要性；面临的风险、安全可靠的关键信息基础设施与可信的信息社会的关系及欧盟在加强关键信息基础设施方面存在的挑战。文件的第二部分核心内容是欧盟各成员国如何增强合作；第三部分是行动计划。

第一部分比较全面地阐述了欧盟在ICT关键信息基础设施方面面临的挑战，包括四个领域：

(1) 各成员国发展的不均衡和缺乏协调；

(2) 对关键信息基础设施需要新的欧洲治理模式；

(3) 缺乏早期预警与应急响应；

(4) 国际合作。

对于第一点，文件认为尽管各成员国在关键信息基础设施面临的网络安全挑战方面均采取了各种措施，但成员国之间的发展很不均衡。首先是纯粹以国家为主体的应对措施带来了跨越整个欧洲边界的“风险碎片”。国家之间的差异以及缺乏系统性的“跨界行动”使得各国的应对措施实施起来效果欠佳。特别是欧盟各国的基础设施相互连接，对于某一个国家而言低风险的安全事件可能对另一个国家而言却恰恰相反。为此，需要各成员国之间形成互利互惠、互谅互让的安全政策，提升整体安全意识。进而从整个欧盟和全球的视角出发，把欧盟的整体政策融入到各成员国自身的安全政策当中。

关于新的欧洲治理模式，文件指出ICT关键信息基础设施的安全可靠性对于各成员国而言提出了特殊的挑战。各成员国在制定政策和敦促关键信息基础设施运营商进行保护方面应当保持统一。然而，另一方面市场经济的机制又缺乏足够的动力来刺激这些关键信息基础设施的私人领域按照国家的要求加大对安全的投入。为了解决这一矛盾，文

件提出了一个“3P 模式(Position, Payment and Performance,即职位、薪酬和绩效)”,即把“公私伙伴”融入到国家层面的政策当中,乃至整个欧盟的框架当中。由于目前欧盟层面尚未将这个模式付诸实践,所以文件建议由 ENISA 来负责实施。

为了达到“全欧盟治理”的目标,文件认为早期的预警及响应将极大提高安全性,然而在这方面各成员国参差不齐,某些国家甚至在其组织机构中缺乏这一环节。更让人局促的是各成员国无论双边或多变机制在预警信息共享和协作方面,也非常落后。此外,对 ICT 关键信息基础设施进行保护的主要手段包括通过仿真和演练,并从中提取战略政策。然而,在欧盟国家当中网络安全演习仍处萌芽,跨境演练更是少之又少。目前,各成员国纷纷成立了自己的 CERT 组织,但这些组织应当加强跨界合作,形成整个欧洲的“计算机应急响应群”。

关于国际合作,文件以 IPv4 向 IPv6 的过渡为例,强调了在互联网这一巨型分布式系统中全球合作应对威胁的必要性。为此,文件提出了两个关键点:首先是根据欧盟自身的优先级考虑向国际社会发出对互联网安全可靠的统一声音;其次,在国际社会商议相关议题的时候,要体现欧盟的核心价值。

上述内容实际上明确了欧盟关于 ICT 关键信息基础设施保护的目标。在确立了这些目标之后,文件给出了各项举措和行动计划。

《关键信息基础设施保护》第二部分“增强各成员国合作”方面,文件提出了五条举措:

(1) 在成员国各个层面做好准备;

(2) 提供足够的早期预警机制;

(3) 加强欧盟对关键信息基础设施的防御机制;

(4) 提升欧盟在国际合作方面的优先级;

(5) 支持“欧盟关键信息基础设施识别与设计实施指导计划”。

在第三部分“行动计划”方面,按照“准备、探测、预警、响应、恢复”这个 PDR (Protection, Detection and Response,即保护、检测和响应)标准流程,再加上“国际合作”,文件共罗列了十三条行动计划。

综上,《关键信息基础设施保护》的主要目标就是解决欧盟各成员国关键信息基础设施互联互通所面临的安全隐患,并对存在的问题提出了具体的措施和方案。

2010 年 8 月 26 日,欧盟又颁布了《数字欧洲计划》[EU2010]。其中也专门开辟了一个章节阐述“可信与安全”,并用如下语句阐明了欧盟对信息安全的观点:“数字时代既不能是‘黑老大’,也不能是虚拟的‘蛮荒西部’”该文件包括五个部分:

(1) 当今网络世界存在的各种犯罪活动,以及可能对公众工作和生活造成的影响;

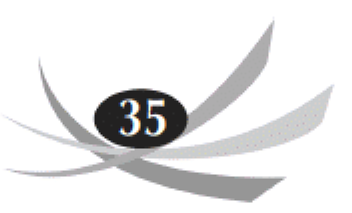
(2) 介绍了提升公众安全意识的重要性以及各成员国应当采取的各项措施;

(3) 欧盟保护个人隐私数据的各项措施;

(4) 保护关键信息基础设施,这一点主要是让公众了解上述《关键信息基础设施保护》计划;

(5) 一系列关键行动,包括成立 ENISA、采取法律措施制止网络攻击、成立欧洲打击网络犯罪平台(2012)等等。

从上述两个战略性文件中,我们可以看到欧盟委员会在应对 ICT 安全的各项挑战方



面已经初步形成了共识,并从2010年开始加大了落实各项政策的力度。

首先从战略层面,除了欧盟主席巴罗佐与奥巴马总统达成欧美在网络安全领域的战略合作意向之外,美国国土安全部长也在2011年4月访问了匈牙利,并与欧盟负责网络安全的主要官员,欧盟内部事务协调官Cecilia Malmstrom及"数字欧盟计划"协调官Neelie Kroes举行了会晤。以协调双方在全球网络信息安全方面的立场。

其次,2010年4月20日,ENISA发布了一份题为《当前和新兴网络技术的研究重点》的报告[RPCE2010],明确指出供应链完整性是未来三至五年内欧洲IT安全研究将重点关注的五大领域之一。

ENISA认为供应链的完整性在信息通信技术行业内是一个重要概念,已经得到了公共和私营部门(例如供应商、基础设施所有方、经营商)的共同关注。"完整性"作为一个概念,和具体的行动、价值、方法、手段、原则、预期和结果的一致性是相关的。"完整性"是安全的一个核心要素。从信息安全的角度而言,完整性意味着数据没有以未授权的方式变更,没有丢失或者被篡改。从软件的角度而言,完整性可定义为确保获取、开发和传递软件的过程包含了增强用户信心的控制手段,让用户确信软件功能如供应商所设计的那样。一般而言,在信息通信技术领域中,完整性是一个复杂的观念,其与确保安全和信任(当系统以预计的方式运行和使用时,我们信任系统)的概念有关。最终目标是提供满足初始规格或者议定规格的信息通信技术产品。

2010年11月由ENISA牵头组织"泛欧网络安全大演习",该演习的重点就是回应上述《关键信息基础设施保护》文件中所提出的问题,包括通过各成员国跨界互动的仿真演习来审核欧盟网络安全政策的可行性、考验各成员国的协同配合程度等。目前这种演习已经开始向常态化方向发展,值得世界其他国家学习。

再次,为了落实《关键信息基础设施保护》中提出的建立覆盖各欧盟成员国基础设施安全保护的应急响应组织,2011年6月Neelie Kroes领导的团队组建了覆盖全欧盟机构的CERT组织,从而将原来隶属各成员国的CERT组织进一步在欧盟框架下进行了整合。

然而,作为一个松散的国家联盟,相比起各主权国家,特别是信息化发达国家,欧盟整体的信息安全架构仍处于探索过程中。造成这种情况的主要原因有两方面:一是各成员国由于自身的战略定位不同而导致对信息安全在国家战略层面上的意识不同;二是以美国为首的北约组织已经为欧盟重要成员国撑起了一把虚拟保护伞,美国对欧盟自身的军事一体化进程也一直抱有戒心,从而导致欧盟自身的信息安全战略及组织架构相对弱化。因此欧盟在制定面向全体成员国的信息安全政策方面也存在诸多问题。

(1) 欧盟在制定网络空间综合性的安全政策方面既落后于美国,也落后于欧盟中的三个发达国家英、法、德。为此,欧盟委员会与ENISA密切合作,协调和指导其他成员国制定相应的信息安全政策,从而整体提升欧盟的信息安全战略水平。

(2) 欧盟《布达佩斯公约》的签署进程即使在其成员国内部也出现放缓迹象。自从2001年开放签署以来仅有27个国家签署,其中8个欧盟成员国奥地利、捷克、希腊、爱尔兰、卢森堡、马耳他、瑞典和波兰颇为迟疑,因为担心数据保护和公民隐私等问题。这些欧盟成员国自身对《布达佩斯公约》的犹豫态度毫无疑问会给世界其他非欧盟国家带来负面

影响。

(3) 在军事层面，北约早已将网络攻击列为最主要的安全威胁之一。2010 年 11 月北约里斯本“新战略概念”中就明确了要应对这种攻击。但北约和欧盟之间的合作并不令人满意。其中最主要的原因在于北约这个美国具有举足轻重发言权的机构与欧盟本身的定位存在错位。

(4) ENISA“心有余而力不足”。2004 年根据欧盟 460/2004 指令成立的这家“欧盟网络与信息安全局”是欧盟各成员国在网络信息安全领域的指导机构。目前它正扮演着越来越活跃的角色。在 2010 年 11 月首次泛欧网络安全大演习之后，ENISA 被欧盟委员会赋予了强制性介入成员国信息安全战略的角色。然而，ENISA 地处希腊的克里特岛，如果倒退到古希腊时代，风景如画的克里特岛倒是不乏哲人大师和斯巴达勇士，但今天它距离欧洲的新中心布鲁塞尔有 2500 公里之遥，难招聘合格的 IT 人才。此外目前 ENISA 有 65 名雇员，也远远不能满足欧盟对信息安全整体战略和诸多具体协调工作的需要。

3.4 英国 ICT 供应链安全战略

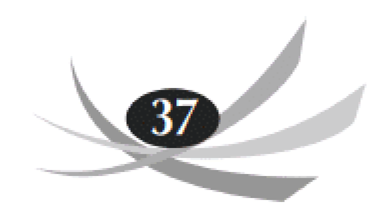
1990 年英国人 Tim Berners-Lee 在欧洲核子研究中心(CERN)发明了万维网，此后，Internet 借万维网之威力，在全世界迅速扩张。同时，英国的网络建设和信息化也飞速发展，总体处于世界先进水平。随后，英国将网络空间作为从事商业活动的重要领域，并达到了相当大的规模。例如，在电子商务方面，B2B、B2C 等领域发展迅速，行业数据咨询公司的最新数据显示，英国的 B2C 电子商务销售总额在 2012 年达到 773.5 亿英镑(约合 1247.6 亿美元)，英国成为全球最大的电子商务市场之一；在互联网普及率方面，英国电信监管机构 Ofcom 发布的数据显示，截止 2011 年年底有 74%的英国家庭在使用宽带网，远超 60%的欧盟平均水平。同时，英国的关键信息基础设施系统，如公用事业、食品生产与配送、运输、医疗保健。

3.4.1 英国 ICT 战略概述

英国对网络空间的高度依赖，也无疑给英国带来了新的风险和威胁。因此，无论是工商业界还是军方与政府都高度重视网络空间的安全。网络空间是当前 ICT 供应链的重要组成部分，网络安全战略直接影响了 ICT 供应链的安全。

2009 年 6 月，英国出台了首个国家网络信息安全战略文件——《英国网络信息安全战略》[COUK2009]，以下简称《2009 战略》。在该文件中，时任英国首相戈登·布朗将网络信息安全战略与历史上英国重要的安全战略相提并论，同时宣布，政府将成立两个网络安全新部门——网络安全办公室(UK Office of Cyber Security, OCS)和网络安全行动中心(UK Cyber Security Operations Centre, CSOC)。OCS 负责协调政府各部门网络安全计划，而 CSOC 的任务则是协调政府和民间机构重要 ICT 系统的安全保护工作，由此也可见政府对其重视程度。

2011 年 11 月，英国政府又公布了新的《英国网络信息安全战略》[COUK2011](以下简称《2011 战略》)，目的是建立更加可信和更具弹性的网络环境，以实现经济繁荣，保障



国家安全及公众安全。

2012年8月，英国内部起草了《通讯数据法草案》[DCDB2012]，以确保执法机关能够及时发现和预警ICT供应链中来自信息网络的威胁。

3.4.2 英国ICT安全战略分析

1.《2009战略》分析

为了应对日益严峻的网络安全问题，英国政府亟待建立一个统一的应对机构并制定战略方针，2009年6月英国出台了该国历史上首个网络信息安全战略文件《2009战略》时任首相戈登·布朗指出："正如19世纪我们必须在海上确保国家安全和繁荣、20世纪在空中确保国家安全和繁荣一样，在21世纪，我们同样必须确保我国在网络空间中的安全，从而给予公众和企业在该领域安全活动的信心。"

《2009战略》有三条主线：降低网络空间风险、利用网络空间抓化机遇、提升对网络安全事件的响应能力。在降低网络空间风险方面，英国将致力于减少漏洞来缓解网络安全事件造成的影响；在利用网络空间抓住机遇方面，英国将综合运用各种搜集的情报，提升国家层面对网络空间敌意行为采取行动的支持力度；在提升对网络安全事件响应能力方面，该文件强调要进一步提高相关的知识与安全意识，完善相关的学说和政策，改进决策机制，加强技术与人员的能力。

该战略指出要加强政府间的跨部门协作以及国际合作。该文件认为，若要确保英国在网络空间的利益、绝非凭借单个部门之力即可实现的，必须建立起一个横跨政治、经济、军事、文化各领域的庞大而又有序的网络安全组织架构，而这个组织架构的建立和有效运转，离不开政府间的跨部门协作甚至是国际合作。3.4.1节提到的CSOC与OCS两个机构的组建即是为了完成这一使命。

该文件认为英国政府应高度重视与私营企业间建立合作关系，重视发挥学术科研机构的优势，同时也应重视培养英国公民的网络安全意识，提高他们维护基础设施安全的自觉性和能动性。

文件中还多次强调，应在防御不法入侵的同时，要主动出击、充分发挥网络空间的优势，对网络犯罪分子、恐怖分子实施打击。

《2009战略》的出台标志着英国政府应对网络空间的威胁迈出了第一步，然而随着网络安全环境日趋严峻，英国政府认为自己已成为来自世界各国的网络犯罪攻击目标，有些攻击甚至具有国家背景。因而，出台更加细化、更加完善的战略举措势在必行。

2.《2011战略》分析

2011年11月英国政府推出了新的英国网络信息安全战略文件《2011战略》。该文件概述了来自其他国家针对英国的敌意攻击以及大规模的网络犯罪活动，并将其作为国家安全面临的首要威胁。英国将在接下来的四年中耗资6.5亿英镑来应对网络威胁，提升该国的网络安全水平。

针对《2011战略》，英国内阁大臣弗朗西斯·浩德说："我们去年发布的国家安全战略已经将网络安全与国际恐怖主义、国际军事危机和自然灾害共同列为首要任务之一，我们的主要目的是让英国成为全球最安全的商业基地。"英国现任首相大卫·卡梅伦表示，

鉴于互联网对于社会、政治和经济增长的重要作用，有必要防范那些威胁网络安全的因素。新战略不仅针对威胁国家安全的恐怖主义分子，也将打击危害公众日常生活的网络犯罪。

《2011 战略》由“网络空间驱动经济增长和增强社会稳定”、“不断变化的威胁”、“英国 2015 年网络安全前景”和“行动方案”四部分组成。

人们注意到，作为美国最亲密的伙伴，在美国发布《网络空间国际战略》之后，英国网络信息安全政策也作了进一步细化和调整，将注意力集中在维护本国网络安全、加强本国网络安全产业竞争力、创造网络安全商业机遇方面在该战略核心的“英国 2015 年网络安全前景”中，短短六十余字中两次提到了“促进经济大规模增长”和“促进经济繁荣”，充分表明了英国政府以网络安全为杠杆来促进经济发展的决心。

文件中表示将加强政府与私有部门的合作，共同创造安全的网络环境和友好的商业氛围，同时报告还提出对中小企业的扶持政策，规定 25%的政府网络安全合同将交给这些最具创造力的企业。

文件中还强调了将与国际社会一道来形成网络空间的国际准则或者路线图，与其他国家一起协作建立可操作的互信机制，从而降低风险升级的可能性和减少误判；同时指出，英国已经批准了“布达佩斯打击网络犯罪的公约”并将和其他国家一道促成配套的法律，从而使得跨界的网络犯罪能够得到审判，避免网络空间成为犯罪分子的天堂。

若把《2009 战略》作为比较基准，可以发现，《2011 战略》有下列突出点。

(1) 更加具有可操作性。虽然立足于维护网络安全，但并不局限于它本身，而是试图通过构建安全的网络空间来促进英国经济繁荣、国家安全和社会稳定。新战略更加强调战略的实施细节，并在附录中详细阐述了针对四个战略目标的具体实施方案。战略实施方案分别从政策导向、执法体系、机构合作、技术培训、人才培养、市场培育以及国际合作等方面提出了实施细则，具有很强的可操作性。

(2) 更加强调国际合作。新战略中提到英国将寻求与那些志同道合的国家，以及那些虽不完全认同但仍可合作的国家，达成伙伴关系，并与包括北约、联合国、欧盟等国际组织的合作，建立可操作互信机制，从而降低风险升级的可能性和误判。

在国际合作方面，英国将美国放在了首要地位。自“二战”以来，英美两国合作密切。在当今风起云涌的国际形势下，英国更将美国视为最亲密的盟友，并发挥其独特的优势以配合美国的 ICT 信息安全战略。特别是近年来，英美两国多次举行了高级别的网络安全演练，这些演练涉及两国核心的政府信息系统，这也表明了英美两国依然保持着深层次信息互通的密切关系。

2011 年 5 月，英国议会正式批准了在 2001 年签署的“布达佩斯打击网络犯罪的公约”。这一举动也体现了英国将与国际社会一道，共同打击网络犯罪活动。

(3) 充分发挥优势，促进英国企业提升在 ICT 安全和服务市场的占有率。赢得海外业务并促进经济增长。文件中提到英国贸易投资总署(UK Trade & Investment，UKTI)将与安全产品领域的贸易协会通力合作，促进英国公司的海外销售。英国将化威胁为机遇，把构建强有力的网络安全转化为所有英国企业的优势，以及英国竞争力优势的一部分，同时，还能够促使英国的网络空间成为其他国家从事商业活动的“避风港”。

3.5　德国ICT供应链安全战略

3.5.1　德国ICT安全概述

德国作为一个开放的社会及现代化的工业化国家，正面临着日益增长的安全需求。2010年7月14日德国内阁通过了由德国联邦教研部主持制订的“2020高科技战略”[HTS2010]，该战略汇集了德国联邦政府各部门的研究和创新政策举措。

2020高科技发展战略较以往更加以人为本，强调技术变革为人类利益服务，因此重点关注5个领域：气候/能源、保健/营养、机动性、安全性和通信。

在安全方面，其强调：“为了保护现代民主社会和关键信息基础设施不受恐怖活动、蓄意破坏、有组织犯罪和自然灾害或意外事故，我们需要新的安全技术来规避危险，并保护重要的基础设施和供应链。决策和行动选项需要安全访问基于空间的技术。除了提供保护免受威胁和创造安全条件，安全技术产品和服务还有助于制定德国具体的职能需求，使德国安全技术领先市场。”

前瞻性项目“有效地保护通信网络”，旨在促进新的、以需求为基础的安全解决方案，符合德国的民主价值观。

相关活动：联邦政府2011年国内安全研究计划如下。

- 开发保护现代民主社会的解决方案：国内安全研究与其他高科技战略领域(保健/营养，通信，气候/能源)的活动有联系。目的是研究新的安全文化和安全架构的概念，并进行更密集的科学和社会对话。
- 开发清晰的职能需求：在此领域，其目的是与最终用户携手合作(公安机关，私营基础设施运营商等)在德国建设新的安全领域，并建立必要的科研基础设施和卓越的研究。我们也希望加强欧盟范围内的合作，并与选定的合作伙伴拓展国际产学研联盟。
- 为规避风险和重要基础设施保护开发新的安全技术：在该行动中，目的是开发风险和威胁的规避和分析(例如早期预警系统，预防的级联效应，仿真工具)工具，并提供系统事件的预防和应对。
- 使德国成为国内安全解决方案的领先市场：目标是制定解决方案，在符合安全的民主理解的前提下在安全与自由之间取得适当的平衡，并定义标准并将其引入全球性的水平。德国是世界公认的在安全技术产品和服务领域有高水平专业知识的合作伙伴。研究和开发资金也更多面向小型和中小型企业，而公共采购更加关注安全技术的创新。

2010年11月，德国联邦经济和技术部发表《德国ICT战略：数字德国2015》，作为指导德国信息通信技术发展的纲领性文件，该战略对德国2010—2015年信息通信技术领域的工作重点、任务和重点项目进行了详细介绍。

德国ICT产业的优势主要体现在软件和嵌入系统方面，但很多人并没有意识到这一点。德国有很多高品质的ICT产品和服务，如欧洲最大的微电子集群德累斯顿生产的半

导体芯片。根据 OECD 预测，德国 2009 年在电子产品生产方面位居世界第五位[ICTS2010]。

德国政府认为 21 世纪是互联网的世纪，维护 ICT 的有效性以及完整性、可靠性和机密性成为至关重要的问题。网络空间包括所有通过互联网进入的信息基础设施，是超国界的。德国社会经济生活领域目前已对网络高度依赖。德国重要的公共基础设施、企业和民众都依赖互联网的信息数据与沟通技术。信息技术产品及其组件出现故障、信息基础设施崩溃或遭到严重的网络攻击，都可能给德国的各个领域造成严重影响。从国内与国际形势看，确保网络安全已成为德国政府、企业和社会面临的重要挑战。这些挑战需要德国政府采取积极的应对措施。

2011 年 2 月，德国又发布了国家网络安全战略[CSSG2011]，旨在保护网络空间安全，提升信息通信技术应用的可信度，促进经济社会繁荣。

《德国网络安全战略》同时对德国面临的 ICT 威胁现状进行了评估，明确了德国网络安全总体形势及其特点。评估认为，鉴于信息基础设施日益增长的复杂性和脆弱性，德国网络安全形势仍然十分严峻，德国公共和私营部门以及整个社会都可能受到信息技术故障的影响。评估明确指出德国网络安全形势的特点：

(1) 近年来对德国信息基础设施的攻击日益频繁复杂，肇事者更加专业，攻击来自德国境内外；

(2) 鉴于网络空间的高度开放，攻击者更有可能利用系统漏洞开展隐秘性攻击；

(3) 应对复杂的恶意软件和网络攻击的技术相当有限；

(4) 通常攻击不会暴露攻击者的身份和背景，也难以找到发起攻击的源头；

(5) 行业信息系统发展的趋势是以标准组件为基础的，并把组件连接到网络空间，这主要是出于经济方面的考虑，因此会产生新的漏洞。对“震网”病毒(Stuxnet)的研究经验表明，重要的工业基础设施也会成为网络攻击的目标。

3.5.2 德国 ICT 安全战略分析

1. 战略框架

《德国网络安全战略》明确了德国确保网络安全的框架条件，即加强国内与国际合作，国内外政策措施兼顾。该战略认为，这是确保网络安全、加强执法和保护重要信息基础设施的需要。首先，在网络世界里，国家、企业和社会责任共担，只有他们像伙伴一样一起采取行动完成任务，网络安全战略才可能成功。其次，信息技术系统是相互关联的全球网络，其他国家发生的信息基础设施事故也可能间接地影响到德国。因此，加强网络安全还需要制定与执行国际行为规则、标准和规范。只有国内外政策措施兼顾，才能真正维护网络安全。网络安全可以通过优化框架条件来得到加强，这一框架条件是与盟友和合作伙伴开展合作的最低标准。打击快速增长的网络犯罪需要全世界各执法当局之间的密切合作。

2. 战略原则

《德国网络安全战略》明确了德国确保网络安全的两项基本原则。

(1) 网络安全必须保证与联网的信息基础设施的重要性以及需要保护的水平相一



致，而且不损害网络空间的发展机会和利用率。网络安全措施既要保障互联网络的畅通与开放，同时又要对重要的信息数据进行有效的保护；哪些设施与数据需要保护或重点保护取决于其重要性；这些措施涉及国家在内、外两个层面所做的努力，以及世界各国的共同努力。

(2) 网络安全必须加强信息交流和合作。该战略一方面主要关注网络安全的民用方法和措施；另一方面，鉴于信息和通信技术的全球属性，它则强调了国际协调的不可或缺。这不仅包括在联合国开展的国际合作，也包括在其他跨国组织中开展的国际合作。国际合作的目的是为了确保国际社会有能力采取一致行动，保护网络空间。

3. 战略目标与措施

德国政府制定网络安全战略的总体目标是大力推动安全网络空间建设，促进德国经济与社会繁荣。基于目前的网络安全挑战，德国政府将以CIP实施计划确立的架构为基础，采取措施，应对当前的威胁。德国政府计划把网络安全措施重点集中在十个战略区域：保护重要信息基础设施、保护信息技术系统、加强行政部门的信息技术系统安全维护、设立国家网络防御中心、设立国家网络安全委员会、加强网络空间的犯罪控制、在欧洲与世界范围内采取有效的协调措施确保网络安全、利用可靠的信息技术、加强联邦主管当局中的人事发展、建立应对网络攻击的工具。这十个战略区域可以归纳为战略目标、战略管理机制、战略保障措施三个层次。

(1) 首先是四项具体战略目标的确立。

① 保护重要信息基础设施。德国政府认为重要信息基础设施的保护是网络安全的重要组成部分。为此，德国政府要求公共和私营部门都必须为更好地利用信息共享、密切协调，创造更好的战略和组织基础。德国政府将进一步加强落实并拓展CIP实施计划的相关规定，强化部门间的合作与整合，扩大新技术的引进范围，并进一步明确哪些部门和基础设施必须采取强制性的保护措施或者在受到特殊威胁的情况下需要额外的保障。在信息技术系统危机期间，德国政府将审查出台协调规则的必要性，以确保重要信息基础设施的安全。

② 保护德国信息技术系统。德国政府认为信息基础设施保护需要提高民众和中小型企业使用的信息技术系统的安全性能。为此，德国政府计划采取如下措施：第一，普及网络安全知识，联合社会团体收集有关信息技术系统风险及安全使用的信息，为用户提供服务；第二，对信息技术产品与服务进行安全标准与使用便捷性的审查；第三，为国家认可的大众使用的基本安全功能(如电子身份证)提供特别激励措施和资助。为了支持信息技术系统安全领域的中小型企业，德国联邦经济和技术部组建了“企业信息技术安全”特别工作小组，邀请企业参加。

③ 加强行政管理部门的信息技术系统安全维护。德国政府要求各级政府必须成为维护数据安全的典范，并决定采取如下措施：第一，计划在联邦政府内建立一个共享统一安全的网络系统(联邦网络)作为电子音频和数据传输的基础，并将继续大力推进联邦政府的实施计划，以应对严峻的信息安全形势；第二，合理配置联邦和地方的资源，将联邦各级政府有力地组织起来，确保信息技术安全；第三，将联邦政府信息安全的联合投资与政府预算挂钩，便于各级政府采取统一行动落实实施计划；第四，由联邦信息技术规划委员

会负责加强同地方政府的合作，尤其是在计算机紧急应对小组方面的合作。

④ 加强网络空间的犯罪控制。德国政府要求各级执法部门、联邦信息安全办公室与私营部门加强打击网络犯罪，防止网络间谍活动。为了促进这一领域的信息交流，德国政府准备在执法机构的参与下成立一个联合机构，发挥咨询顾问的作用。面对日益增长的全球网络犯罪活动的挑战，德国政府将做出巨大努力，以欧洲理事会《网络犯罪公约》为基础，实现打击网络犯罪活动的全球协调。

(2) 其次是统一的战略管理机制的形成，并明确责任机构和协调机制。

① 设立国家网络防御中心。为了加强各级政府之间的合作，提高协调应对信息技术系统突发事件的能力，德国政府计划设立国家网络防御中心。

它将向联邦信息安全办公室汇报工作，并直接与联邦宪法保护局、联邦公民保护和救灾办公室合作。联邦刑警局、警察局、海关犯罪刑侦总署、情报局、国防军以及负责重要基础设施运行的各级部门，在他们法定任务和权力框架内参与该中心的工作。

国家网络防御中心的主要任务是，根据网络攻击的形式尽可能确认攻击来源，对网络安全突发事件做出缜密的分析，并为统一行动提供可靠的建议。国家网络防御中心将定期就日常的基本预防和特定事件向国家网络安全委员会提交建议。网络安全危机迫在眉睫或已发生时，国家网络防御中心将直接通知由联邦政府内务部以国务秘书为首的危机管理人员。

② 设立国家网络安全委员会。德国政府认为识别及清除危机产生的体制性因素是预防网络安全问题的重要手段。因此，德国政府希望建立和保持联邦政府内部的合作以及联邦政府信息技术特派员负责的公共和私营部门之间的合作，特别设立国家网络安全委员会。这个国家网络安全委员会包括联邦大臣和国务秘书，国务秘书分别来自联邦外事办公室、内务部、国防部、经济科技部、司法部、财政部、教育科研部以及各州的代表，特殊情况下还会包括其他部的代表。委员会还会邀请商业代表作为特邀会员参加委员会的工作，必要时也会邀请学术界的代表参加。委员会的主要任务是负责协调预防性工具与公共和私营部门网络安全方法的交叉问题，统一协调联邦政府层面的信息技术管理问题，从政治和战略高度统一协调信息技术规划委员会在网络安全领域的工作。

③ 加强国际协调与合作，在欧洲与世界范围内采取有效的协调措施，确保网络安全。德国政府认为全球网络安全只有在国内及国际的层面通过协调工具才能较好地实现。在欧盟方面，德国政府支持采取基于行动计划的适当措施来保护重要信息基础设施，根据变幻的 ICT 安全形势以及欧盟机构内部信息技术能力的汇集，适当扩大欧洲网络与信息安全局(ENISA)的授权；依照欧盟内部安全战略和数字议程开展进一步的网络安全行动。在塑造德国的外部网络安全政策方面，德国政府将有关网络安全的利益和想法通过国际组织中协调和执行，如联合国、欧安组织、欧洲委员会、经合组织和北约。德国政府认为日益多元的办法必须与主权评估和决策权保持一致，为此建议出台由多数国家签署的国家网络行为准则，其中包括建立信任的安全措施。在八国集团框架内，德国正在加紧反僵尸网络活动。德国政府支持北约新战略关于建立统一的安全标准的承诺，北约各成员国可以在自愿的基础上使用这一标准来保护民用重要基础设施。

(3) 最后是对具体的保障措施的确定。

① 加强技术保障。为了确保信息技术系统及其硬件设施长期安全可用,德国计划大力支持促进网络安全的创新保护计划。为此,德国政府将继续加强对信息技术安全以及重要基础设施保护的研究;强化德国的科技知识产权,全面加强信息技术核心战略能力尤其是经济能力建设,将其列入德国的政治策略;与合作伙伴尤其是欧洲的盟友共同集合德国的相关资源。

② 加强联邦政府与各州政府之间的合作,推出应对网络攻击的工具。德国政府认为要想充分应对网络攻击,必须与各州政府合作,建立一套全面协调的工具。德国政府将继续定期评估网络安全状况,并采取相应的保护措施;还将根据需要对是否有必要赋予联邦其他的法定权力进行相关审查。

③ 加强联邦网络安全人员的培训。

4. 德国 ICT 安全战略的特点

(1) 注重网络安全顶层设计。在《德国网络安全战略》中,德国联邦政府明确设立网络安全战略目标,国家成立相应的负责机构,把网络安全纳入国家安全战略之中。在最高层设计下所确立的网络安全战略目标,成为其他原则、措施制定的依据和基础。该战略确立的网络安全战略目标,即确保德国 21 世纪的互联网的安全,促进德国社会经济繁荣发展,成为框架条件、两项基本原则、四项具体目标、具体的管理运行机制以及其他相关保障性措施的统领。它所阐明的所有措施、手段、管理、技术、法律等,都是围绕其战略目标所设计的。

(2) 重视国内资源整合,通过机构设置,加强国内合作与协调。这一点在框架条件中有明确阐述。该战略重视各级政府部门之间、公私部门之间、用户与企业之间、政府部门与企业及学术界的交流合作,并成立专门的网络安全防御与管理机构,统一协调各部门之间、公私部门之间、企业与用户之间在维护网络安全方面的冲突与联系。德国政府将进一步加强落实并拓展 CIP 实施计划的相关规定,强化公私部门间的合作与整合;通过设立网络安全防御中心协调联邦政府与地方各级政府部门间的职责关系;通过网络安全委员会的设立,协调联邦政府内部各部门与私营部门之间的职责关系。由此,形成了国内相对完善的覆盖政府各级部门与私营部门的网络安全防御管理与运行机制。最后,该战略明确表示其所确立的目标、机制和机构必须通过联邦、各州政府和企业长期合作,才能真正实现。

(3) 重视国际战略合作。通过支持与参与国际相关规则的制定,加强国际合作与协同。促进国际与国内网络安全的协调。这一点由框架条件所确立,也这为网络空间跨国界的特性所强化。该战略明确认识到网络空间的超国界属性,网络安全维护的复杂性与多变性,因此尤其重视网络安全维护的国际合作,这在其框架条件、基本原则以及具体的战略措施中都有体现。该战略在其框架条件中明确指出,确保网络安全,加强执法权和保护重要信息基础设施都需要加强国际合作;加强网络安全还需要制定与执行国际行为规则、标准和规范;只有国内外政策措施兼顾,才能真正维护网络安全;框架条件是制定与盟国和合作伙伴共同利益的最低标准。该战略的两条基本原则也体现了对国际合作与协调的重视,尤其强调网络安全需要全面的理解,不仅要有民事、军事的预防措施,更要有国际

层面的相互合作，以保证国际社会的正常运转，维护网络安全。在战略目标与措施方面，该战略明确表示要加强国际协调与合作，在欧洲与世界范围内采取有效的协调措施，以确保网络安全。如前所述，德国政府将与欧盟各国通力合作，推进欧盟内部安全战略与数字议程；依据欧盟的《网络犯罪公约》规则指导，打击网络犯罪行动；遵循多元的办法与主权评估和决策权一致的原则，确立国际网络行为准则，指导国际网络安全合作；支持八国集团反僵尸安全计划行动，支持北约有关网络安全的规定；积极参加国际网络安全治理。

（4）重视战略的防御性。与美国、俄罗斯、英国相比，德国的网络安全战略强调防御性，从技术、管理人员等方面着手，防范黑客对德国网络进行攻击，加强网络安全。西方大国尤其是美国组建网络司令部，组建网军，研发网络攻击武器（并进行了实战），采取进攻姿态，保护网络安全。德国没有组建网军，也没有像美国那样宣布发起网络攻击将引发美国的导弹攻击报复，而是将重点放在民用网络安全方面的防御，重点打击网络犯罪。这一点把德国限定在是一个“文明国家”的范围内。与此同时，德国也以军民分离的形式保留着发展军事网络安全战略的空间。

（5）重视战略的灵活性与适应性，根据情况进行定期审查与修改。该战略的总体目标是确保网络安全与德国的自由与繁荣。该战略并不认为这是一蹴而就的事情。德国政府认为能否达到这一目的，在很大程度上取决于德国能否以国际一流的有效措施来保护网络空间。由于信息技术革新周期短，网络空间的技术性与社会性也会发生变化，德国政府将定期审查检验在国家网络安全委员会全面控制下网络安全策略的目标是否取得了成功。德国政府还将根据框架条件以及现实需要调整未来的网络安全战略及其措施[CQH2011]。

3.6 法国 ICT 供应链安全战略

作为欧盟的创始国之一和欧洲大陆的传统强国，目前法国的人口数和经济总量在欧盟各国中均排名第二，仅次于德国。截止 2010 年，法国家庭互联网用户为 74%，高于欧盟的平均水平。而企业互联网用户高达 97%，也高于欧盟的平均水平。在安全意识方面，74%的个人用户经常使用专用工具保护自己的数据和计算机系统，也高于欧盟 59%的平均水平。然而，在企业信息化的安全政策方面，法国却以 22%的水平低于欧盟 26%的平均水平。事实上，这个数据从某种程度上也反映出法兰西民族在信息安全领域现实与政策发展不均衡。（数据来源：欧盟统计局网站，http://epp.eurostat.ec.europa.eu）。

3.6.1 法国 ICT 安全概述

从公开发布的资料来看，法国政府直到 2008 年 7 月才在《法国国防与国家安全白皮书》[FWP2008]（以下简称《2008 国防白皮书》）中，将网络信息安全提升到国家安全的层面。法国参议院也在同一时间发布了一份名为《网络防御与国家安全》的报告，其核心内容与《2008 国防白皮书》大致相同。

2011 年 2 月，法国国防与国家安全总秘书 Francis Delon 授权“法国网络与信息安全局”（French Network and Information Security Agency，ANSSI）颁布了法国历史上第一份国家信息安全战略报告《信息系统防御与安全：法国战略》[ISDS2011]（以下简称《法国

战略》)。

3.6.2　法国ICT安全战略分析

2008年时任法国总统Nicolas Sarkozy授权发布了《2008国防白皮书》。该书全文共335页,分为4大部分18个章节。该文件在第一部分"从全球化到国家安全"第二章专门阐述了网络空间的安全挑战,并将"重大的网络攻击"与"恐怖主义"、"导弹威胁"等相提并论。在概述了现代社会对信息系统的依赖、世界网络安全发展趋势、主要国家的网络战斗能力等等内容之后,该文重点介绍了法国对网络空间攻防作战的认识,并特别提到:"法国需要发展网络空间的战斗能力"。文中还专门阐述了网络空间的作战策略、人员培训和武器装备等方面的初步构想。

对于法国的信息安全战略而言,《2008国防白皮书》最主要的作用就是正式将其纳入了国家安全的总体框架,从而为下一步制定专门的信息安全战略确定了基调。

在机构设置方面,《2008国防白皮书》提出了必须成立一个由总理府领导的网络与信息安全部门,以取代以往层次较低的"国家信息安全指挥中心"。

2009年7月7日,根据《2008国防白皮书》的要求,法国正式成立了隶属总理府的"法国网络与信息安全局"(ANSSI),该局由"国防与国家安全总秘书处"直管。2010年7月,Sarkozy总统宣布将全法信息系统的防御职责也一并移交给该机构,进一步增强了它的职权。目前,ANSSI的核心职能包括:

(1)探测网络攻击并对其进行前期处置(由下属的网络防御行动中心负责),并采取相应的防御机制;

(2)为政府和企业提供可信的产品与服务;

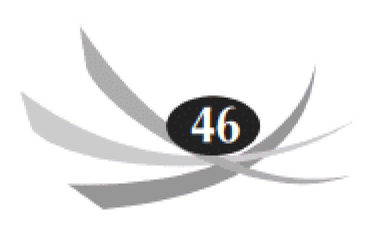
(3)为政府和关键信息基础设施运营单位提供可靠的咨询;

(4)对企业和公众进行信息安全培训、发布相关安全信息和政策。此外,还负责对密码设备及相关服务进行监管等工作。

2011年2月,ANSSI授权发布了法国首份国家级信息安全战略文件《信息系统防御与安全:法国战略》(以下简称《法国战略》),作为对《2008国防白皮书》的响应。

《法国战略》全文25页,为法国的信息安全路线图制定了4大战略目标和7项具体举措。

四大战略目标依次是:"成为网络安全强国"、"保护主权信息,确保决策能力"、"国家基础设施保护"和"确保网络空间安全"。《法国战略》的首要目标是成为与美、英等国齐肩的网络安全强国。尽管保持国防、外交政策的战略独立性是戴高乐总统留给法国人的政治遗产,但自从萨科奇总统带领法国又重回北约的怀抱之后,这种超然于世的独立性已经在悄然发生改变。同时由于网络空间无边无界、瞬时穿越的独有特征,使得法国政府更加体会到"首先要搭上头班车,才能争当驾驶员"。而要成为网络安全强国的逻辑分析也非常简单:《法国战略》认为起因有三:一是外国政府主导的,针对法国国防、科技、经济、商业等重要领域的网络间谍活动危害了法国的主权;二是恐怖主义利用网络空间传播激进思想;三是国家或恐怖组织可能对法国的基础设施发起网络攻击。因此,法国必须成为网络列强之一。只有进入网络安全的第一阵营,才能从高手之间在战略实施层面和操作层



面的合作交流中获益，比如盟国之间在漏洞信息情报的实时交换、防护机制和方法的交流等等：“法国将与它最密切的盟国（特别是欧盟）和国际组织加强网络安全政策方面的国际合作”。

《法国战略》的第二个目标是确保自身的决策能力以及为此所需的敏感信息，其本质是要掌控信息安全核心技术，特别是以密码技术为代表的基础性技术。该文件指出，首先要确保首脑机关在进行决策的时候通过保密信息系统获得相关的信息资源。为此，要大力发展密码技术及相关产品的研发能力，以及密码分析能力。这也是确保法国国家战略独立性的要求。

中世纪以来，法国数学家名满天下，创下了世界数学发展史的半壁河山。法国人在世界密码技术上也具有值得骄傲的历史。即使不把大名鼎鼎的凯撒密码算成法国密码学的始祖，在中世纪的欧洲，法国人发明的 Vigenere 密码也在西方密码学历史上留下了辉煌的一笔，再加上“二战”法国参与破译德军 Enigma 密码的诸多经验、教训，以及遭受的窝囊气，使得法国政府对现代密码技术的认知更加刻骨铭心。当然，强调密码技术在法国信息安全国家战略中的核心地位还有一个重要原因，那就是法国政府赋予了 ANSSI 关于密码技术和产品监管的职能。

除了确保政府重要部门对保密信息的技术需求之外，该文件还提出要将这需求向下延伸，保证地方政府以及基础设施运营单位对密码产品的需求。

《法国战略》的第三个目标是“保护国家基础设施”在法国的“国防法案”中对基础设施的定义是：对公众生活、国家权力机构的运行、经济活动、国防能力和国家安全具有不可替代的领域。该文件指出：“随着多种技术的融合，真实世界和虚拟空间正在交互。真实世界的许多事情现在都通过网络连接起来，这就使得控制这些物体成为可能……目前，这些基础设施都通过网络相互联系。而绝大多数工业界的人士缺乏对 IT 系统的了解，反之亦然。众多利益有关方现在都通过网络互联。服务外包、云计算、实时管理等等。正如世界新闻媒体报道的那样，人们尚未对针对工业控制自动化系统的恶意攻进行充分的评估。因此这些问题与保护通信网络一样，已经成为国家优先考虑的问题。”由此可以看出法国政府对网络攻击未来发展趋势的高度重视。从某种意义上讲，震网病毒对提升世界各国政要的信息安全意识功不可没。

《法国战略》的最后一个目标是“确保网络空间的安全”文件再次勾勒了网络空间中的各种犯罪活动以及可能给公众带来的损失之后，强调要从安全意识培养与法律制约两个层面来保护网络空间安全，包括建立有关安全评估的发布渠道；提升现有的法律框架，使其与虚拟社会的发展相匹配；加强国际司法合作等。

纵观《法国战略》的 4 个目标，涉及了加入世界信息安全第一梯队的雄心、强调核心技术自主研发能力、国家社会经济命脉的保护和安全意识提升及法律框架的改进等方方面面。而尽管这 4 个战略企图并未像美国政府那样鸟瞰全球，引领潮流，但却根据法国自身特点进行了量身定制。有所为有所不为。

为了落实上述战略目标，文件接下来罗列了 7 个具体行动。

1. 跟踪与分析

文件要求对各种新技术、新产品、新标准进行跟踪分析，甚至要深入参与到各个公私

领域的有关活动当中。

2. 探测、预测和响应

由于社会经济生活对互联网的高度依赖性，因此必须能够探测安全漏洞、尽快填补它们、及时通知潜在的受害者，并为它们提供相应的方案。为此，文件提出三条具体措施：

(1) 按照《2008国防白皮书》的规划，发展探测网络攻击的能力，并把这种能力配置到各部门的信息系统当中，将使得相关人员能够及时预警，并采取相应的措施。

(2) 多渠道实时获取国家网络状态的安全信息。并且在有必要对危机进行干预的时候，由ANSSI下属的作战指挥室(Operationroom)应对这些挑战。

(3) 授权ANSSI指挥整个国家的信息系统防御。

3. 提升并保持安全能力

文件要求提升法国的科学、技术、工业和公众的安全能力，并持之以恒。文件具体要求：

(1) 继续发挥法国在“形式化方法”和“密码技术”等方面享誉全球的优良传统，而在信息系统安全构架方面“要迅速赶上最先进的国家”，为此，法国正在审议建立一个网络防御研究中心，以及探讨与工业界在网络防御科研领域合作的可能性，这个中心将进行各种科研活动，包括密码研究，攻击行为分析、恶意代码分析专家、开源的安全软件开发、网络防御概念的凝练等等，以及从事专业人员的培训。

(2) 通过加大国家战略性投资，提升法国国内的工业基础，确保信息安全产品的研发生产能够留在国内，防止供应链攻击。

(3) IT的设计者要在其开发的前期就将安全问题考虑其中，以提高系统设计的效率。而在法国的工业基础产业中，信息安全专业人员，特别是年轻人才也要相应的增加。在通识性的科学技术和信息技术课程当中，也应当包括信息安全课程。

4. 保护国家信息系统及关键信息基础设施

《2008国防白皮书》要求法国必须掌握和开发高端安全产品来保护国家秘密，并且为政府部门和各个领域提供可信赖的产品与服务；还要采用可靠安全的网络，用于核心决策，确保指挥链畅通。为此，文件提出以下4条举措：

(1) 由于法国已经重新加入到北约军事一体化进程当中，因此法国对于承载涉密信息的安全产品和组件重新做了定义，使其产品能够与其他成员国之间进行互操作，确保北约内部“军令畅通”。

(2) 在政府各部门的网络中采用认证技术，特别是法国引以为傲的智能卡技术来改善整体安全。

(3) 除了继续使用现有的政府安全内网之外，在2012年还将为决策层配置个拥有加密系统的电话网络和一个安全的视频系统。此外，这些安全方案还将在推广到下面的政府机构当中。

(4) 建立政府与私营领域有效的合作沟通机制来保护关键信息基础设施的安全。首先，通过这个机制，利益相关方将获得由国家层面获取和分析的重要情报；其次，允许国家权威机构介入对基础设施的保护。

5. 法律对虚拟社会的适应性

该文件认为要从法律的角度关注网络空间中的各种活动。既要考虑对个人自由的影响,也要考虑国家社会生活的正常运行。因此法国的司法体系必须适应当今的技术发展。要重新审视各种法律法规,以考察各种新技术渗透到社会各阶层时法律的适应性,确保国家利益。文件提出的具体措施包括:

(1) 将欧盟有关信息安全的指导性意见融入法国法律,从而更好地保护信息系统,使得政府能够预警和处理危机。

(2) 增强和不断发展"总体安全框架",将使得政府部门不断提升信息系统的安全,增强与用户之间的关系。

6. 拓展国际合作

法国将与各国政府加强信息交换,特别是关于产品漏洞信息方面。法国还将加强在打击网络犯罪方面的国际合作。文件认为,与盟国之间在网络防御政策的合作是法国的基础。法国正在仔细考虑与精心挑选的可信赖的合作伙伴在操作层面进行更加深入的合作。

7. 安全意识

文件认为关于信息安全政策的辩论对公众、社会乃至国家安全的影响至关重要,但法国尚未充分开展这方面的讨论。为此,文件提出:

(1) ANSSI 将为国家有关决策层提供相关的辩论议题;

(2) ANSSI 还将为大众及公司举行政策宣贯。

《法国战略》是法国政府迈向国家网络信息安全战略的第一步。从这个文件预留的空间中可以预测今后法国信息化发展和信息安全保障工作将不断迈上新的台阶,进一步完善属于法国人自己的网络信息安全学说。

3.7 俄罗斯 ICT 供应链安全战略

3.7.1 俄罗斯 ICT 战略概述

俄罗斯作为前苏联解体后的主体国家,在世界两级格局中也曾是发达国家,尽管现在的俄罗斯以发展中国家的角色自居,但跻身或说重回世界强国阵营一直是俄罗斯国家战略的重点,因此其信息安全领域的战略审计同样重视网络能力、信息通信技术水平在国际社会的排名。

近些年来,俄罗斯在面临传统威胁的同时,在信息通信技术安全方面又面临新的威胁。例如,外国敌对势力利用信息基础设施等技术手段进行渗透;国际恐怖分子利用互联网进行恐怖活动;国内的犯罪分子利用计算机进行犯罪活动等。此外,还把信息对公民心理的影响和外国媒体在俄罗斯的无控制传播纳入到信息安全范畴。

为了应对信息安全威胁,俄罗斯在方针政策、组织机构、法律等方面采取措施,提高信息安全的保障能力。

2008 年,俄罗斯联邦总统梅德韦杰夫批准了两份文件:《俄罗斯信息社会发展战略》

和《确保俄罗斯联邦信息安全的措施》。在这之前，俄罗斯政府还曾批准《为教育开发统一信息环境(2001—2005年)联邦计划》(2001年)、《信息技术用于联邦组织机构的概念》(2004年)以及一项名为《电子俄罗斯》的联邦计划(2005年)和一项名为《2007—2011年国家技术基础》的联邦计划(2007年)。

2009年5月12日，俄联邦总统梅德韦杰夫批准了《2020年前俄罗斯国家安全战略》第537号文件[NSSRF2009]。战略的第109款明确指出，在实现安全战略过程中，保障免受信息安全威胁，要提高俄罗斯联邦信息通信系统和关键信息基础设施以及高风险设施的安全性、提高公司和个人信息系统的保障水平、创建统一的信息通信系统以支撑安全系统。

1. 俄罗斯信息安全纲要

2000年9月9日生效的《俄罗斯联邦信息安全纲要》是旨在强化国家信息安全政策的《国家安全概念》(2000年1月10日由总统批准)的扩展。纲要的出台旨在帮助俄罗斯从法律、方法、技术和组织方面为信息安全作出规定，同时帮助为达到这样的目的制定出具体计划。纲要从信息角度定义了国家利益，评价了公民、社会乃至整个国家面临的威胁。纲要论述了政策涉及的诸多方面，从数据保护、个人隐私、版权和计算机滥用(黑客攻击)，到国家机密、访问信息和控制媒体，称得上非常全面。

纲要把俄罗斯的信息安全定义为“在平衡个人、社会和国家总体利益的基础上定义的信息领域保护国家利益的状态”。俄罗斯把公民的心理和国家信息系统同时视为信息安全概念不可分割的组成部分。此外，外国新闻媒体在俄罗斯无控制的传播被看作是对俄罗斯信息安全构成的威胁之一，因此，政府意图“强化”俄罗斯媒体的作用[JNTA2009]。

纲要依照俄罗斯联邦有关安全的法律阐述了国家机密、信息保护和参与国际信息交流等问题。纲要共分4章11节，各章的主要内容如下：

信息安全：本章定义了信息领域的俄罗斯联邦国家利益，阐明了宪法赋予的权利、信息对国家政策的支持、信息业的发展以及防范未经授权访问的信息保护。本章还确定了俄罗斯信息安全所受威胁的内部和外部来源。纲要坦诚地承认，与私人垄断和有组织的犯罪一样，政府的政策和立法也会构成一种威胁。富有侵略性的外国公司和国际恐怖分子被称为主要外国威胁。在国内方面，国家工业的关键性以及正在完善中的法律框架对信息技术的充分利用形成了一种障碍，这在电子商务方面表现得尤为突出。最后，本章讨论了俄罗斯联邦的信息安全现状以及改进的目标。涉及国家机密的数据的安全状况恶化被确定为一个主要问题。

确保信息安全的方法：本章阐明了关键信息基础设施保护的法律、组织——技术和经济方法。此外，它还描述了信息安全在经济、国内政策、外交政策、科学和技术、信息和电信系统、国防、执法和紧急情况等诸多方面的特点。最后，本章介绍了信息安全领域的国际合作如禁止信息武器、支持信息交流、协调执法活动、预防对涉密信息的未经授权访问等确保信息安全的国家政策的主要规定以及需要优先执行的措施：本章高度概括地阐明了从遵守宪法到支持新技术开发的政府政策。本章提议了有关信息安全的规定，如为联邦机构拟定指南等。此外，本章还阐述了落实法律规定、提高国家领导的效率、制定访问信息档案的计划、系统培训、统一计算机化和信息安全标准等优先措施；确保信息安全

的组织基础；本章描述了信息安全系统的功能，以及包括总统、联邦议会、联邦理事会、联邦议会国家杜马、俄罗斯联邦政府、安全理事会以及其他联邦行政当局、总统委员会、司法机构、社会团体和公民在内的俄罗斯信息安全系统的组织元素和参与者。

纲要着重强调的一个方面是，为信息安全创建一个法律基础。《俄罗斯联邦宪法》、《国家机密》、《信息、计算机化和信息保护》、《参与国际信息交流》等法律在纲要中具体描述。法律工具构成了实现纲要所述信息安全的三大手段之一，另外两个手段是组织——技术措施和经济措施。

2. 电子俄罗斯

“电子俄罗斯”的概念最早出现在2001年初，当时经济发展和贸易部在为俄罗斯制定截至2010年的战略发展计划。这个计划所基于的理念是，为了缩小经济差距，必须发展高技术部门，使其达到比原材料部门更高的生产水平。如果没有计算机和强有力的信息和通信技术，这一目标根本不可能实现。

涉及联邦政府各部并由电信和信息化部（该部后于2004年改名为信息技术和通信部）负责协调的《2002—2010年电子俄罗斯》是一个核心IT计划，它将为通过大规模推广信息和电信技术提高经济和政府管理效率打下坚实基础。该计划还旨在通过技术手段推动民用机构保护公民限制信息访问的权利以及增加培训专业人员和合格用户的机会。

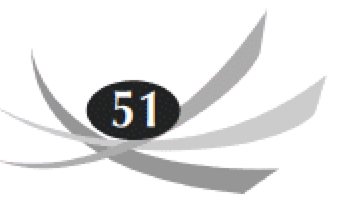
“电子俄罗斯”有一个9年规划期，主要涉及5个重要方面：监管环境、机构框架、互联网基础设施、电子政务、电子教育。

“电子俄罗斯”的主要目标是提高经济的效率、改善公共部门的管理，以及通过应用信息和通信技术加强自我管理。为了达到这个目标，必须完成以下任务：制定有效的ICT立法；确保国家实体、机构和公司之间通过应用先进ICT技术开放交流和互动；为更广泛和更高效地把ICT应用到经济和社会生活之中创造条件；为专业人员提供最新的计算机培训；制定方案推动独立的新闻媒体把ICT应用到专业活动中；发展电信网络基础设施，为公民、国有组织和教育机构访问电子图书馆、档案、科学技术信息数据库提供便利；支持国家采购和其他商业活动实现电子商务化。

2006年，俄罗斯联邦政府修改了这一计划的部分目标和任务。“电子俄罗斯”计划的主要目标最初仅限于通过在政府部门使用信息和电信技术以提高政府员工使用IT的技术水平和改进政府为公民服务的质量来提高政府行政管理的质量。如今，“电子俄罗斯”有了一个主要针对电子政务问题的4年规划期。

“电子俄罗斯”现在的主要目标是通过应用信息和通信技术提高公共部门的管理效率。为了实现这个目标，必须完成以下任务：提出有关在政府部门使用应用信息和通信技术的标准和建议；通过信息和通信技术以及政府部门信息系统的集成提供不同部门之间的有效互动；应用控制政府部门活动的信息系统；开发软件和技术解决方案，用以支持政府部门的活动；监督计划的落实。

“电子俄罗斯”计划的地区性分支之一是“电子莫斯科”城市计划。这项宣布于2002年12月24日的计划旨在强化莫斯科作为俄罗斯信息业中心的角色，该计划建立在该市强大的电信基础设施——“莫斯科光纤网”上。“电子莫斯科”提出的问题包括为信息社会构建标准化和法制化基础，提高市政管理的水平并实现电子政务，发展城市经济并克服本市



的信息不平等，构筑具有高度互用性的框架，将市政当局所有现行ICT项目融为一个整体。

3. 国际合作

国际合作是俄罗斯联邦信息安全保护领域的一大重要成分。俄罗斯在这方面的国际合作有两个独有的特点：争夺技术和信息资源以及称雄市场的国际竞争愈演愈烈；世界列强已经取得越来越大的技术领先优势，这使它们具有创造“信息武器”的潜力。俄罗斯极为关注这种发展状况，因为这会在信息领域引发一轮新的军备竞赛，加大外国情报机构通过特务和利用全球信息基础设施等技术手段渗透俄罗斯的威胁。因此，俄罗斯联邦信息安全领域的国际合作主要涉及以下方面：禁止发展、扩散和应用“信息武器”；确保国际信息交流的安全，其中包括通过国家电信渠道传送的信息的安全；在世界范围内协调执法机构的活动，开展反计算机犯罪的斗争；禁止未经授权访问国际银行、电信网络和信息支持系统中赖以维持全球贸易的保密信息；与国际执法组织共享信息，打击有组织的跨国犯罪、国际恐怖主义、麻醉品和精神药品的非法交易、武器和核燃料的非法交易和人口贩卖；俄罗斯积极参加活跃在信息安全领域的所有国际组织，其中包括标准化和认证组织。

根据2003年12月8日联合国大会第58/32号决议，一个信息安全联合专家组成立，由俄罗斯的一位代表担任组长。该联合专家组由来自15个国家的代表组成。此外，俄罗斯政府还与上海合作组织(Shanghai Cooperation Organisation，SCO)成员国和集体安全条约组织(Collective Security Treaty Organization，CSTO)成员国在信息安全领域建立了合作伙伴关系。

3.7.2　俄美ICT安全战略对比

俄罗斯和美国是当今国际政治的核心成员，在网络空间领域也是重要的利害关系人。但是双方因为语言、国情和文化背景等等各方面的不同，自然对网络的理解不同，对使用网络的目的、方式以及欲达之效果也不同。于是，找到美俄达成共识的相关要素与适当路径，才能够为制定有效的国际网络行为准则奠定基础。2011年，美俄相关机构以“第二轨道外交”的方式对有关网络安全的20个基础性概念进行了界定及解释，并将其视作两国间此类合作的有效开端。

遗憾的是，这次互动起步就不顺利，双方在多个概念上的差异与分歧陷入僵局。首先是战略“标的”的确定，俄方选择“信息安全”，包含信息的各个方面和所有形式，而不能仅限于作为信息载体“次领域”的网络。但是美方强调网络所包含的只是“数据”，所以只能在网络空间的框架内讨论“网络安全”。两国还在“网络冲突”和“网络战争”等等概念上存在理解上的差异。英语中的网络冲突意指(民族国家)或有组织团体之间或多个(民族)国家或有组织团体内部因不受欢迎的网络攻击引发报复行为而形成的紧张局面。但是俄语解释为国家或有组织的集团和组织内部的紧张局面，是由于敌对的(不受欢迎的)网络攻击行为激发(导致、使产生)的反应。二者区别在于：(1)英语的“国家”指代具有民族性，而俄语没有此语意；(2)俄语拿“敌对的”来对应英语中的“不受欢迎的”；(3)英语的“报复”一词，俄语界定时候也用了“不受欢迎的回答”来对应。类似于上述的理解偏差在20个概念中还有很多，无论这些不同是因为两种语言之间转换的必然存在，还是美俄双方观

念上的分歧,这一尝试总是为启动构建国际网络安全规范做出巨大贡献。

俄罗斯作为前苏联解体后的主体国家,在世界两极格局中也曾是发达国家,尽管现在的俄罗斯以发展中国家角色自居,但跻身或说重回世界强国阵营一直是俄罗斯国家战略目标的重点,因此其信息安全领域的战略设计同样重视网络能力、信息技术水平在国际社会的排名。另一个方面,两极时期的美苏争霸留给俄罗斯的依旧是美俄关系的对抗和意识形态的冲突。从现实主义的角度分析,美俄关系的恶化,势必带来军事上的对峙,加强军备竞赛是后果之一。而美国将网络空间的防卫力量和传统军事进行关联,俄罗斯信息技术的发展完全可能被美国认为是军备竞赛的手段和措施,这种判断会反作用于美俄关系走向异常,强烈影响国际秩序的稳定和发展。美俄关系变化将直接反作用于中俄、中美关系,会影响中国战略发展机遇期的持续,关系到中国地缘政治环境、能源环境和外交环境,需要密切关注。

3.8 澳大利亚ICT供应链安全战略

澳大利亚是世界上最早制定互联网管理法规的国家之一。澳大利亚政府十分重视国家ICT基础设施的保护、网络身份和隐私的保护以及灾难恢复能力的建设,建设有严密的安全系统和防范措施,注重调动全社会的积极参与、注重信息安全测评体系建设、注重国际安全合作。

3.8.1 澳大利亚ICT战略概述

在最新的《网络安全战略》出台之前,澳大利亚政府已经在ICT安全领域进行了一系列部署,制定并采取了一系列的政策和措施。

1999年,澳大利亚政府发布保护国家信息基础策略,采取五点策略保护国家信息基础设施。

2000年,澳大利亚政府发布了信息安全风险管理指南,为信息安全风险管理过程的建立和实施提供通用指南。

2003年,澳大利亚建立关键基础设施保护计划,加强ICT关键基础保护。

2006年,澳大利亚通信与媒体管理局(Australian Communications and Media Authority, ACMA)制定澳大利亚互联网计划,帮助用户解决“僵尸”计算机问题。

2007年,澳大利亚政府理事会开始制定和实施国家网络身份安全战略,加强公民网络身份的安全性,保护个人身份。

2008年,澳大利亚政府承诺在四年内斥资1.258亿美元施行全面的网络安全计划,以对抗网上风险,帮助儿童父母和教育工作者保护未成年人免受不健康信息侵扰。同年,澳总理在向国会提交的《国家安全声明》[NSS2008]中提出,网络威胁是澳大利亚面临的头等国家安全问题之一。

2009年7月,澳大利亚政府发布了《澳大利亚数字经济未来发展方向》报告[ADEFD2009],认为网络信息安全是其实现为所有公民提供最大限度从数字经济中获益的目标的关键因素。



2009 年 11 月，为进一步加强网络和信息安全，澳大利亚政府出台了《网络安全战略》[AG2009]。

2010 年，澳大利亚政府发布《ICT 可持续发展计划 2010—2015》，旨在帮助财务管理和问责法案 1997 机构，使其能够适应政府 ICT 的使用的海外可持续发展议程。通过关注 ICT 设备的采购、安装、维护、使用和处置，政府的目标是更有效地利用 ICT 资源，提高效率，提高生产率，并降低其 ICT 业务的环境影响。该计划确定了 ICT 产品和服务的政府采购适用标准，并采取措施提高 ICT 环境绩效，特别是在能源效率方面。ICT 可持续发展计划的另一个重点是政府机构有效利用 ICT 技术，促进政府、行业和社会各界进行更多的可持续实践，以保障整个澳大利亚经济和社会效益。

2013 年 1 月 23 日，澳大利亚政府发布其首份《国家安全战略》[SAN2013]，其战略目标中明确指出，要加强澳大利亚的人员、资产、基础设施和机构的弹性。具体包括加强主要部门的信息共享，更有效地整合国家安全、社会和经济政策，加强各国政府间合作并与私营、非营利机构和社会各界一起应对潜在攻击，与国家关键基础设施团体建立伙伴关系等。

3.8.2　澳大利亚 ICT 战略分析

2009 年澳大利亚的《网络安全战略》分析了澳大利亚 ICT 领域面临的网络安全挑战，指出澳大利亚的国家安全、经济繁荣和社会安康极大地取决于信息和通信技术（ICT）的可用性、完整性和保密性，明确提出澳政府网络安全政策的愿景是维护一个安全、恢复力强、可信的电子运行环境，以支持澳大利亚的国家安全，经济的收益最大化。

战略认为澳政府网络安全政策制定应基于以下六项指导原则：

- 网络安全复杂性需要国家强有力的领导。
- 所有用户应该共担责任，采取合理步骤来加强自己的系统安全，并有责任尊重他人的信息和系统。
- 澳各级政府、私营部门以及社会团体之间要形成合作伙伴关系。
- 鉴于互联网跨国境的本质，澳大利亚应积极主动、多层面地参与网络安全领域的国际协作。
- 所有连接互联网的系统都具有潜在的脆弱性，并且网络攻击可能难以检测，必须采取基于风险的方法评估网络安全。
- 在制定网络安全政策时，除了考虑加强个人和整体的安全，还应注意保护澳大利亚人民的隐私权和其他基本的价值观。

《网络安全战略》提出了澳大利亚政府网络安全政策的关键目标，并阐述了为实现这些目标而确定的战略重点。澳大利亚政府网络安全政策提出三项关键目标。

- 目标一：让澳大利亚所有公民都意识到网络风险，确保其计算机安全，并采取措施保护自己的网络身份、隐私和资产。
- 目标二：澳大利亚各个行业可使用安全和恢复力强的信息与通信技术，加强供应链管理，来保护其运营的安全，以及用户的网络身份和隐私。
- 目标三：澳大利亚政府确保其信息和通信技术是安全和恢复力强的，能对抗

风险。

基于上述三项关键目标，战略提出 7 个优先项。

(1) 威胁意识与响应——提高探测、分析、消减和响应网络威胁的能力，重点关注政府、关键基础设施和关系国家系统利益的其他系统。

具体措施包括：在国防部建立网络安全运行中心(CSOC)，提供 24×7 式网络安全情境感知能力，协调对网络安全事件的响应；建立新的国家 CER_T，共享信息，加强政府与私营部门间在应对网络安全威胁时的有效协调；积极参与并推动国内、国际政府与企业内部及政府与企业之间可信、及时的信息共享，确保网络安全情境感知能力的维护和对在线威胁的全球一致响应；更新网络安全风险管理计划，提出国家重大网络安全事件的响应部署纲要，包括各州、各区以及私营部门的协调合作；指导开展网络安全演习，以测试事件响应部署的有效性，包括与美国合作开展“网络风暴”系列演习。

(2) 文化变革——向澳大利亚全民进行在线自我保护的教育，为他们提供信息和实践工具，增强其信心。

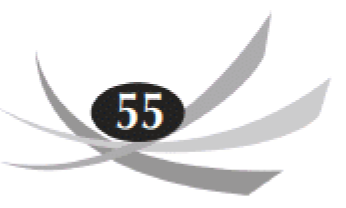
具体措施包括：为家庭用户和小型企业建立权威的网络安全知识网站；建立澳大利亚 CERT，确保澳大利亚网络用户能够获取关于网络安全威胁、系统安全漏洞以及如何更好地保护信息技术环境方面的信息；提供实践工具；在澳大利亚中小学开展网络安全的单元课程教育；与企业、用户群体、社会组织等伙伴一起，继续实施“网络安全意识周”计划；研究如何将各种网上风险，包括网络安全、身份安全、网上诈骗信息有效地告知并教育互联网用户。

(3) 政企合作——与企业伙伴共同推动提升基础设施、网络、产品与服务的安全性与恢复力。

具体措施包括：通过 CERT 加强与私营部门的互信伙伴关系，共享网络威胁、脆弱性及其潜在后果方敏感信息；推动商务网络企业提升网络安全意识，识别网络威胁和脆弱性，采取适当的风险消减策略；通过关键基础设施可信信息共享网(The Trusted Information Sharing Network for Critical Infrastructure Resilience，TISN)推动企业提升网络安全和关键基础设施保护的最佳事件；通过实施关键基础设施保护建模与分析(The Critical Infrastructure Protection Modelling and Analysis，CIPMA)计划，为企业和政府提供世界领先的计算机建模能力；通过与国际政府和教学机构的协作，为企业代表创造教学和培训机会。包括在工业控制领域关键系统相关工作的人员；与澳大利亚标准协会(Standards Australia)和其他企业实体共同制定和推广最佳网络安全实践标准；确保安全问题在澳大利亚国家宽带网络的设计和运营阶段就进行考虑和处理。

(4) 政府系统——树立政府 ICT 系统(包括与政府进行网上交易的相关系统)保护的最佳实践。

具体措施包括：研究降低澳政府网络网关数量的途径，将实际数量降到最低，以便将高效性、可信性和安全性最大化；建立更有效的跨政府部门最低安全标准，要求所有主要政府部门的 ICT 项目开展网络安全评估；与各州、各地方，其他关键利益相关者共同促进政府系统的有效安全保障；对《澳大利亚政府防护安全手册》(Australian Government's Protective Security Manual)进行评估，确保其信息安全政策和标准能够与技术发展保持



同步并能反映国际最佳实践。

(5) 国际参与推动形成一个安全可信、可恢复且能为澳大利亚国家利益提供支持的全球ICT供应链环境。

具体措施包括：与盟友或共识国家就网络安全合作达成双边或多边协议；建立区域论坛，重点关注区域内部的能力建设计划；通过国际组织退工国际最佳实践，发展和形成一种协调的全球路径以对抗网络安全威胁；制定一项国际参与战略，明确界定和描述澳大利亚在网络安全与社会福利方面的国家利益和优先任务。

(6) 立法与执法——维护有效的立法框架和执法能力，依法治理网络犯罪。

具体措施包括：为安全和执法机构提供额外资源，增强打击网络犯罪和其他网络安全威胁的行动能力；确保网络安全与打击网络犯罪的执法工作之间的有效联结；与各州和地方政府合作，确保澳大利亚有关法律能够与技术和犯罪行为的发展保持同步；向澳大利亚法律专业人士提供必要程度的技术支持和对有效执行相关法律的充分理解；促进澳大利亚网络安全的法律框架与司法权限相协调，在国际上推动信息共享和跨境执法合作。

(7) 知识、技能与创新——推动成熟网络安全人才的发展，研发创新性的安全解决方案。

具体措施包括：实施招募和保留策略，确保专业技术人员在政府机构的充分发展；通过一些像"国家安全项目研究支持"这样的项目，为网络安全研发活动提供目标明确的支持；每年设定一套研发优先任务，并广泛向科学与创新共同体告知哪些优先工作符合政府网络安全政策要求；本工作将通过澳政府的"国家安全科学与创新战略"推动实施，该战略确定网络安全提升澳大利亚国家安全的12个科学与创新优先领域之一。

3.9 各国ICT供应链安全战略对比

纵观各国的与ICT供应链相关的战略，凸显出以下几个共同特点。提升战略认识，赋予网络空间或信息通信供应链以国家战略意义，在实质上确定了信息通信供应链安全对于维护国家安全利益的直观重要性。实行内部整合，强调通过政治、军事、经济、执法、外交、技术等各种力量和手段保护网络空间安全；强调部门之间的集中整合、力量配合，公共部门和私营部门的合作，以及所有利益相关方的合作。强化技术支撑，重视技术体系的建设，突出确保政府网络、国防网络及关键信息基础设施安全这一"保核心、保重点、保要害"的战略思想。注重自主可控，强调保证信息技术全球供应链的安全。倡导国际合作，积极推动国际合作并谋求制定信息通信供应链的国际规则和规范。各国战略文件均不同程度地从战略认识、组织结构、能力构建、安全保障、国际合作、管理理念等多个不同层面表达了对维护国家信息通信供应链安全的愿景。

细览各国战略，从总体内容结构上看也大有相似之势。一是各国战略都立足与本国信息技术发展水平，对本国网络空间和信息通信供应链当前态势进行基础调研和环境分析，其重点无外乎是对当前的网络威胁走向和信息环境未来的前景进行判断。在此基础上界定本国网络安全/信息安全建设的基础。二是各国战略都将保护本国关键基础设施作为安全第一要务，将其作为保障国家政治稳定和经济发展的基础，视为国家根本利益的

维护和保障。第三，战略目标明确。根据各国战略文件中对于网络安全建设目标的表述，基本可以归纳为：建设一个“开放、平等、安全、健康”的网络空间环境，抵制网络犯罪、网络攻击等国际性网络危害行为。各国通过各自阶段目标的安排设置进度，期待最终实现这一国家战略目标。第四，世界各国都普遍认识到，在网络空间这个或虚或实的领域确实需要秩序和管理，各个国家都在呼吁并寻求国际合作和全球治理的途径与方法。

当然，由于各国的国情不同，国内信息化程度也有差别，所持有的信息技术优势又不尽相同，因此各国战略的重点迥然各异。首先，以美俄为代表的两个信息大国在国际网络领域的讨论“起点”上存在分歧。美国是互联网技术的领跑者，自然也是网络技术相关概念的创造者，比如网络空间、网络对抗等。而这些英语的新创词汇，必然会导致不同语言之间缺乏“自然等值体”与之对应，出现理解上的差异。美国将“网络空间”解读为“支撑我们日常通信的相互依存的信息技术组件，互联网是网络空间的一部分。”很明显，美国有着互联网技术和资源优势，更愿意将相关的设施、技术纳入战略管束之内，因此美国对“信息”的解读更偏重“物质性”——即网络所包含的是“数据”，于是倾向于把战争对象界定为“网络安全”。

但是，在此问题上俄方坚持认为讨论的起点应当是“信息安全”。俄方认为这样能够涵盖信息的各个方面和所有形式，而不应仅限于只规划“作为信息载体‘次领域’的网络”。因此，俄罗斯为战略定名为《俄罗斯联邦国家“信息社会”纲要》。俄方强调，信息包括经过加工和未经加工的资料；网络是由人类“加工”而成的，这一本质特征也就决定了存在于网络中的数据同人脑以及书籍、文献中的资料一样，都是信息，所以应当在“信息安全”的框架内加以讨论。在战略题名中出现“信息”而不是“网络空间”的法国既主张通过互联网向意识形态不同的国家推广“民主”、“自由”的西方价值，又提出“文明网络”防范美国通过《网络可信身份国家战略》导致的“同化”。可见法国战略的“独立性”是基于其技术上的先进性和对国际治理主导权的期待，因此法国式战略与美战略故意有所区别也体现出其对美国战略的警惕。

其次，各国战略宣誓内容也体现了这些国家参与全球网络空间战略博弈的不同立场。对于美国的传统盟友而言，英国、澳大利亚、加拿大的战略中体现了与美国密切合作的主体思路，还将网络空间安全防御内容添加到本国与美国传统的军事合作协议中，如《澳新美安全条约》。至于欧盟国家，虽在网络防御领域与美国合作密切，却未保持整体上一致。其合作的一面体现在2010年创建的“欧美网络安全与网络犯罪工作组”，欧盟美国联手打击网络犯罪，并借助北约平台与美国共同维护网络安全，形成对俄罗斯的防范性遏制。其“不一致”的方面却在深化，欧盟倾向于选择包容性广的全球治理模式，多次建议美国让出对互联网域名管理权的独揽，尽管美国通过外交手段化解了这一欧美争议焦点，但并不能从根源上打消欧盟的顾忌。法国力主向全球推广自己的互联网管理理念，期待带领欧盟摆脱对美国技术的依赖，打破美国互联网企业的垄断地位。其“独立”战略透露出其对全球网络治理主导地位的觊觎，因此推断，法国虽明言发展重点是网络防御，但其信息技术的研发趋势必是进攻型技术导向。

再次，各国战略的公开程度各有不同。比如美国“在关键基础设施的保护”的措施面讳莫如深，只是明确表示“采取积极防御，更加有效地阻止和击败对国防网络信息系统的攻击入侵”。英国、法国、德国等国战略的公开多是追随于此。这类战略篇幅相较简短，都

是纲领性条款，没有实践性内容，由此推之，这些国家在ICT供应链安全方面应该还有更为细致的未公开计划或措施。

最后，各国战略都强调“防御和保护”，但明显有“进攻型”和“应对型”之分。“进攻型”以美国为最，依借其本身在信息技术上的垄断和对国际网络资源的优势占有，美国在《网络空间军事行动战略》、《网络空间国际战略》中提出“美国将使用一切必要手段防御至关重要的网络资产，美国保留诉诸武力的权力”。与美国不同，其他国家则相对弱势，但法英德日等信息技术发达国家引领意图较强，偏向于前者，其他国家更侧重防护，偏向后者。

通过各国战略对比分析，可以看到双边和多边关系之间的微妙变化和更综合层面的问题。可见各国最共同的关注重点还是在“对本国基础设施的保护”——各国共同认为关键基础设施一旦遭到破坏，会对国家产生难以估量的重大影响和损失。

当前，我国面临的ICT供应链安全形势十分严峻，一方面是在信息安全域，别国给我们施加的压力越来越大，我国面临的来自国外的网络攻击不断增多；另一方面，我们的工业基础设施比较落后，自主可控的安全保障能力不足，国家针对信息通信供应链安全战略和全局统筹的机制还没有形成。因此，加快推进信息化建设，建立健全ICT供应链安全全保障体系，加强统筹协调和顶层设计，切实增强供应链安全保障能力，维护国家安全是时代对我们提出的要务和赋予的使命。在未来ICT供应链安全发展战略布局中，我们还要不断地借鉴和学习，对世界各国战略内容进行全局把握和深入分析，客观全面地掌握国际ICT供应链安全态势特点和趋势，做好本国ICT供应链管理，保障我国的供应链安全。

参考文献

[PDD63] Whitehouse. PRESIDENTIAL DECISION DIRECTIVE/NSC-63：Critical Infrastructure Protection. 1998.

[AGDC2007] Australian Government. Department of Communications，Information Technology and the Arts Managing IT Security When Outsourcing to an IT Service Provider：Guide for Owners and Operators of Critical Infrastructure. May 2007.

[NSPP2003] National Strategy for the Physical Protection of Critical Infrastructures and Key Assets，2003.

[GNSS2000] Whitehouse. National Security Strategy in Globalization. 2000.

[EFNMASC2012] World Economic Forum. New Models for Addressing Supply Chain and Transport Risk. 2012.

[BAH2009] Booz Allen Hamilton. ICT Supply Chain Assurance：An IATAC State-of-the-Art Report. 2009.

[CONSS2009] Cabinet Office，U. K. The National Security Strategy of the United Kingdom：Update 2009.

[CA2009] US. Cybersecurity Act of 2009. 2009.

[FWP2008] 2008 French White Paper on Defence and National Security. 2008.

[ISDS2011] Information systems defence and security-France's strategy Anssi. 2011.

[NSPP2003] National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. 2003.

[NISTSP800-53] SP 800-53：Recommended Security Controls for Federal Information Systems and Organizations.

[NIST SP 800-59] Guideline for Identifying an Information System as a National Security System.

[NCSRDC2009] National Cyber Security Research and Development Challenges. 2009.

[BCSCRM2009] Building A Cyber Supply Chain Assurance Reference Model. 2009.

[CTNS2010] Cyber Threats to National Security：Countering Challenges to the Global Supply Chain. 2010.

[CISSP2010] CISSP. Supply Chain Risk Management and the Software Supply Chain. 2010.

[DHSSI2009] Department of Homeland. Security Information Technology Strategic Plan 2009—2013. January 2009.

[DHSDOD2007] DHS，DOD. Defense Industrial Base Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan. May 2007.

[RPCE2010] Research Priorities of Current and Emerging Network Technologies. 2010.

[EOSWP2010] EOS ICT. Cyber Security Working Group An EOS White Paper：Towards a concerted EU approach to cyber security. September 2010.

[HPSCI2008] HPSCI，HPSCI. White Paper on Cyber security. 2008.

[ISWG2009] EOS ICT Security Working Group. Security And Resilience Of Information And Communication Technology Networks For The Protection Of Critical Infrastructures. November 2009.

[IATAC] IATAC，ICT. Supply Chain Assurance：An IATAC State-of-the-Art Report. 2010.

[MD2010] Ministry of Defence，UK. DEFENCE ICT STRATEGY. October 2010.

[COUK2009] Cabinet Office of UK. Cyber Security Strategy of the United Kingdom—safety，security and resilience in cyber space. 2009.

[DCDB2012] Draft Communications Data Bill. Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty. June 2012.

[NARE2011] National Association of Research and Educational E-Infrastructures "E-Arena"，Updated Report about the ICT R&D Priorities in Russia. 2011.

[NCSR2009] National Cyber SecurityResearch and Development Challenges. 2009.

[RP2012] U. S. Resilience Project Cyber Supply Chain Risks，Strategies and Best Practices. January 2012.

[USSA2006] United States Senate. An Assessment of U. S. Efforts to Secure the Global Supply Chain. 2006.

[ICTS2010] ICT Strategy of the German Federal Government. Digital Germany 2015，Federal Ministry of Economics and Technology (BMWi). 2010.

[CSSG2011] Cyber Security Strategy for Germany. 2011.

[WHNSS2010] The White House. US National Security Strategy. May 2010.

[HTS2010] High-Tech Strategy 2020 for Germany. 2010.

[AG2013] Austrilian Government. Strong and Secure：A Strategy for Australia's National Security. 2013.

[NSS2008] National Security Statement. 2008.

[NSSRF2009] National Security Strategy of the Russian Federation to 2020，Decree of the President of the Russian Federation. No. 537，2009.

[ADEFD2009] Australia's Digital Economy. Future Directions. 2009.
[SAN2013] Strong And Secure. A Strategy for Australia's National. 2013.
[ZXD2010] 左晓栋.美国政府IT供应链安全政策和措施分析.信息网络安全.2010.
[CQ2010] 程群.美国网络安全战略分析.太平洋学报.2010.
[CQH2011] 程群,胡延清.德国网络安全战略解析.德国研究.2011.
[JNTA2009] 江南天安.国外基础设施保护俄罗斯篇.信息网络安全.2009.

第 4 章 ICT 供应链安全模型

4.1 概　　述

如今 ICT 供应链面临着各种各样的威胁，某些威胁的破坏性是巨大的，甚至是无法估量的，相关组织和机构有必要采取有效的应对措施来消除或者最大限度地减少 ICT 供应链安全风险。本章总结了国际上最新的供应链安全模型并阐述了各个模型在保护 ICT 供应链安全领域的应用，包括供应链运作参考模型（Supply Chain Operations Reference model，SCOR）、ICT 供应链确保参考模型（Cyber Supply Chain Assurance Reference Model）、普华永道-供应链安全维度模型（Pricewaterhousecoopers-Supply Chain Security dimension model）、NIST 系统开发生命周期模型（System Development Life Cycle，SDLC）、达沃斯-供应链和运输风险模型（Davos-Supply Chain and Transport Risk Model）、ICT 供应链风险管理集群框架（The ICT SCRM Community Framework），为相关组织机构提供了 ICT 供应链风险管理的工具。

供应链运作参考模型（SCOR）是由国际供应链协会（Supply-Chain Council，SCC）开发并授权的供应链管理方法。它是第一个标准的供应链流程参考模型，是涵盖了所有行业的供应链的诊断工具。它能使企业间准确地交流供应链问题，客观地评估其性能，确定性能改进的目标，并影响今后供应链管理软件的开发。其基本思路是将业务流程重组、标杆管理及最佳业务分析集成为多功能一体化的模型结构。

ICT 供应链确保参考模型是由美国科学应用国际合作组织（Science Applications International Corporation，SAIC）和马里兰大学史密斯商学院供应链管理中心在 2009 年共同提出的。该模型表现为由三个嵌套的环组成的过程系统，这三个环分别代表了计划和操作控制的不同层面，用以解决系统开发生命周期中的深度防御需求和网络供应链中的广度防御需求。

供应链安全维度模型是普华永道（PWC）在 2011 年底发布的《运输和物流 2030 卷四》[TLSSC2011]中提出的，目的是为了应对全球化背景下的供应链安全问题。它根据关键绩效指标法（KPI）和可以开展行动的时间范围，从五个方面对供应链安全进行了综合考虑。

普华永道（Price Waterhouse Coopers）是四大国际会计师事务所之一，主要服务领域包括审计、税务、人力资源、交易、危机管理等。普华永道通过制定解决方案及提供实用性意见，不断为客户及股东提升价值。普华永道致力于提供切合各行业所需要的审计、税务及咨询服务，以提升客户的价值。普华永道在 154 个国家和地区超过 161 000 人的专业

团队所组成的全球网络内，对22个行业进行专业研究，分享其思维成果，行业经验和解决方案，并为客户开拓新视野及提供实用的建议。

NIST系统开发生命周期模型是由美国国家标准与技术研究所(National Institute of Standards and Technology，NIST)在其出版物NIST SP 800-64[NIST2008]中提出的。模型首先描述了大多数信息系统开发中关键安全角色和职责，然后将安全措施纳入系统开发生命周期(System/Software Development Life Cycle，SDLC)的各个阶段。

达沃斯-供应链和运输风险模型是在2011年的世界达沃斯论坛上提出的降低风险的策略，用于进一步开发和阐明行动建议。供应链和运输提供者需要在采购、运输和分销等多个环节管理风险。在相互联系的世界上，安全、可靠和高效只能依靠行业及政府之间的合作来实现。从恐怖主义、天气、货币到信息技术的弊端，该模型提供了汇集不同风险的框架，用以帮助政府或者企业定义风险的优先级。

ICT供应链风险管理集群框架是由马里兰大学斯密斯商学院将已有的行业和公共部门的措施应用到不同的ICT段(软件、硬件、网络和系统集成服务)从而提出的模型，能够将在单个风险框架中定义的不同进程和实例结合起来。在美国总统的《国家网络安全综合计划》(Comprehensive National Cybersecurity Initiative，CNCI)的第11项倡议的提议下，美国国家标准技术协会(NIST)为了支持ICT领域的供应链风险管理的发展，负责联邦的相关政策的制定。为了支持NIST的工作，马里兰大学的斯密斯商学院在2011年8月被授予进行开展相关调查和研究并提出该模型。

这些模型不仅可以应用到供应链风险管理的实践中防患于未然，更重要的是它们从不同角度提供了供应链风险管理的思路，值得在实践中借鉴和应用。

4.2　供应链运作参考模型

4.2.1　模型的产生背景

过程参考模型将著名的流程重组，标杆管理和过程测量的概念集成到一个统一的跨职能框架中，如图4-1，量化同类公司的运作性能，根据最好的性能来建立本公司的内部目标。

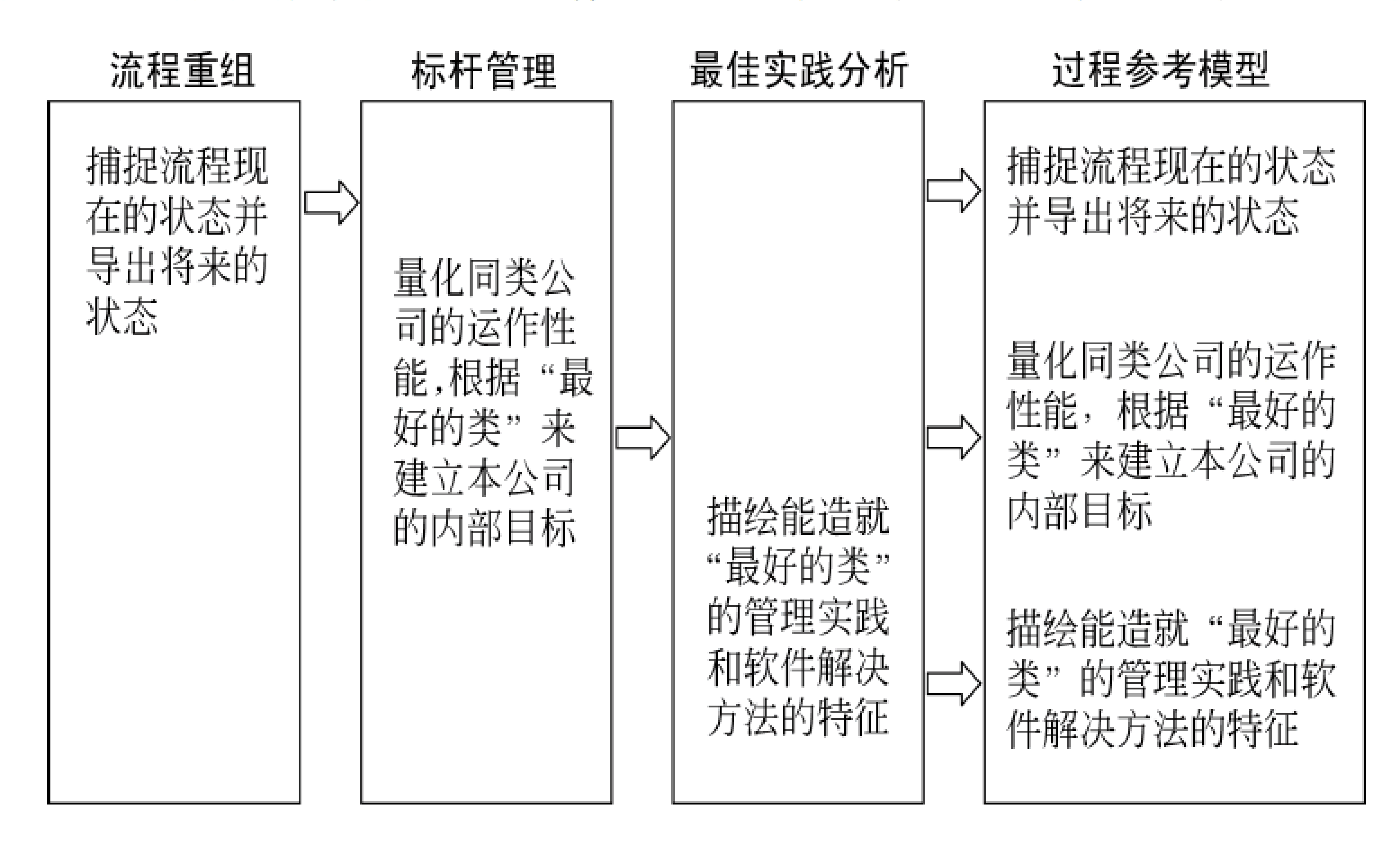


图4-1　过程参考模型[SCC2005]

流程重组 BPR 的产生并不是偶然的，企业的组织机构大都是基于职能部门专门化管理，专业化分工通过分工使劳动者成为某一方面的专家，使处理某一问题的单位效率提高，但专门化分工也带来许多环节衔接问题，与专业化分工相适应的金字塔形组织体系适合稳定的环境、大规模的生产、以产品为导向的时代，但把任务分裂为多个环节，造成部门之间衔接中的大量等待，延长了任务所花费的时间，用某个环节使用计算机软件并不能彻底改变这种低效率问题，MIT 的 Hammer 指出，传统流程的计算机化并没有带来预期效益，原因之一是没有触及传统管理模式。因此必须进行业务流程重组［WZ1］。

1990 年，《哈佛商业评论》杂志发表了迈克尔·哈默（M. Hammer）的文章《改造工作：不要自动化，而要推翻重来》，哈默批评了企业在改造中常犯的错误，即运用信息技术加速已落后了几十年（甚至几百年）的工作流程，指出要对流程进行重新思考，并提出了改造的七项原则。随后哈默与担任 CSC Index 管理顾问公司董事长的 James Champy 于 1993 年合著《再造企业——管理革命的宣言》一书，书中阐述了这一理论：现代企业普遍存在着“大企业病”，面对日新月异的变化与激烈的竞争，要提高企业的运营状况与效率，迫切需要“脱胎换骨”式的革命——业务流程管理，从而掀起了世界性的 BPR 研究浪潮。BPR 的核心思想是要打破企业按只能设置部门的管理方式，代之以业务流程为中心，重新审计企业管理过程，企业应是流程型组织［WZ2］。

美国施乐公司一直保持着世界影印机市场的实际垄断地位，但是 1976 年以后它遭到了来自国内外尤其是日本竞争者的全方位挑战。佳能、NEC 等公司以施乐公司的成本价销售产品并且能够获利，同时产品开发周期缩短 50％、开发人员减少 50％，这样使得施乐公司的市场份额从 82％锐减至 35％。面对竞争者的威胁，施乐公司开始向日本企业学习，开展广泛而深入的标杆管理。施乐公司通过对比分析寻找差距，调整战略和经营策略并重组流程，通过一系列的努力施乐公司取得了非常优秀的业绩，把失去的市场份额重新夺了回来。施乐公司大范围地推广标杆管理法，并选择了 14 个经营同类产品的公司进行逐一考察，找出了问题的症结并采取相应措施。随后，摩托罗拉、IBM、杜邦、通用等公司纷纷仿效施乐公司采用标杆管理法，在全球范围内寻找行业内外管理实践最好的公司进行标杆比较并努力超越标杆企业，它们也成功地获取了竞争优势。此后，西方企业开始把标杆管理法作为获得竞争优势的重要思想和管理工具，通过标杆管理来优化企业实践，提高企业经营管理水平和核心竞争力［WZ3］。

为了帮助企业实施供应链管理，1996 年春，美国波士顿 Pittiglio Rabin Todd& McGrath（PRTM）和 AMR Research（AMR）这两家咨询公司为了帮助企业更好地实施有效的供应链，实现从职能管理到流程管理的转变，牵头成立了供应链协会（Supply Chain Council，SCC）。SCC 选择了一个参考模型，经过发展、试验 、完善，于 1996 年底发布了供应链运作参考模型——SCOR，SCC 将供应链看作描述和改进运作过程效率的工业标准，建立了 SCM 系统的整体框架和流程的细节，还将当前最重要的管理改进方法——业务流程再造（BPR）、标杆（Benchmarking）和最佳实践分析集成在一起作为实施供应链管理的指导。

4.2.2 模型的基本原理

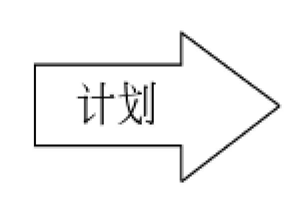
供应链运作参考模型 SCOR 是由国际供应链协会（SCC）开发并授权的供应链管理方法。它是第一个标准的供应链流程参考模型，是涵盖了所有行业的供应链的诊断工具。

它能使企业间准确地交流供应链问题，客观地评估其性能，确定性能改进的目标，并影响今后供应链管理软件的开发。其基本思路是将业务流程重组、标杆管理及最佳业务分析集成为多功能一体化的模型结构。

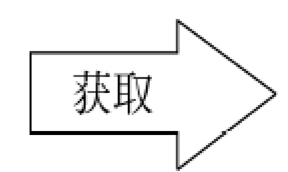
SCOR是以流程为核心的参考模式，包括三个关键要素：框架——借助一套公认的定义，将供应链模块化；性能指标——提供测量供应链绩效的指标；最佳实践（Best Practices）——提供供应链运作改进的标杆。借助一套公认的定义，无论是多简单或多复杂的供应链，都可用SCOR的流程模拟模块来描述，从而将完全不同的行业联系起来。SCOR的实现过程可分为流程模拟、度量指标和最佳实践三个步骤[LHH2009]。

1. 流程模拟

SCOR包括5个独特的管理流程（如图4-2）：计划（Plan）、获取（Source）、制造



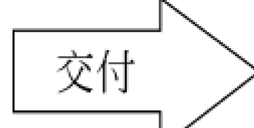
需求/供应计划和管理
› 平衡资源与需求并为整个供应链建立/沟通计划，包括返回、采购、制造和传送；
› 业务规则管理，供应链性能，数据收集，存货，固定资产、运输，规划配置和监管要求以及依从性；
› 协调供应链单元计划与金融计划。



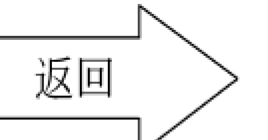
备货生产，按订单生产，按订单设计产品的采购
› 交货时间表，接收、验证和转移产品；授权供应商付款；
› 识别和选择供应来源；
› 管理业务规则，评估供应商表现，维护数据；
› 库存管理，固定资产，传入产品，供应商往来，导入/导出需求，供应商协议。



备货型生产，按订单生产，按订单设计产品的生产
› 安排生产活动、宣传产品、生产和测试、包装、发行产品；
› 完成按订单设计产品的工程；
› 管理规则，性能，数据，进程中的产品，设备和设施；
› 交通，生产网络，遵循生产法规。



备货型产品、按订单生产产品和按订单设计产品的订货、仓储、运输和安装管理
› 从处理客户问询和报价到选择装运商的所有订单管理步骤；
› 从接收和挑选产品到装载和运输产品的所有仓储管理；
› 在客户现场接收和验收产品，如果有必要则进行安装；
› 为客户开具发票；
› 管理交付业务规则、性能、信息、成品库存、苦丁资产、运输、产品生命周期和进入/输出需求。



原材料的返回和成品返回的收据
› 所有返回的缺陷产品的步骤，包括从采购到识别产品状态。处理产品，请求产品返回授权，安排产品出货，返回缺陷产品，交付，授权的产品返回，安排返回回执，接收产品，转移不合格产品；
› 所有返回维护、修理和彻底检修产品的步骤，包括从采购到识别产品状态，处理产品，请求产品返回授权，安排产品出货，返回维护修理操作后的产品，交付，授权产品返回，安排返回回执，接收产品，转移需要维护修理操作的产品；
› 所有返回的多余产品的步骤，包括从采购到识别产品状态，处理产品，请求产品返回授权，安排产品出货，返回多余产品，交付，到授权产品返回，安排返回回执，接收产品和转移多余产品；
› 管理返回业务规则，性能，数据收信，返回目录，固定资产，运输网络配置，遵从法规要求。

图4-2 SCOR管理流程[SCC2005]

(Make)、交付(Deliver)和返回(Return),目的是提供度量供应链绩效的标准方法,以及使用一套公认的度量尺度与其他企业进行比较。

如图 4-3 所示,SCOR 模型按照流程定义可分为三个层次,每一层次都可用于分析企业供应链的运作。在第三层以下,企业将流程要素分解,开始实施特定的供应链管理实践,这些层次中的流程定义不包括在 SCOR 模型中。在这一阶段,企业确定实践措施,以实现竞争优势并适应变化的经营环境。

	层次描述	原理图解	阐释
供应链运作参考模型	1. 顶层	计划 采购 制造 交付 返回 返回	该层定义了供应链运作参考模型的范围和内容,设定了竞争绩效目标的基础
	2. 配置层		公司的供应链可以在该层从30个核心“流程类别”实行定制。企业通过为自身供应链选择的配置来实施各自的经营战略
	3. 流程元素	P1.1 P1.2 P1.3 P1.4	该层定义了公司在它选择的市场中的成功竞争力,包括: • 流程元素定义 • 流程元素信息的输入和输出 • 流程性能指标 • 可应用的最佳实践 • 需要支持最佳实践的系统能力 • 系统/工具 在该层微调经营战略
不在范围	4. 实施层		在该层公司实现了具体的供应链管理实践,定义了获取竞争优势和适应不断变化的业务条件的实践

图 4-3 SCOR 模型的三个层次[SCC2005]

第一层描述了五个基本流程:计划、获取、制造、交付和返回。它定义了供应链运作参考模型的范围和内容,并确定了企业竞争性能目标的基础,是企业建立竞争目标的起点。

第二层配置层(如图 4-4):由可以构成供应链的多个核心流程组成。企业从该层中

定义的标准流程单元中选择他们需要的来构建实际的或者理想的供应链。每一种产品或产品型号都可以有它自己的供应链。

计划
P1 计划供应链
P2 计划采购
P3 计划制造
P4 计划交付
P5 计划返回
供应链
采购
S1 采购库存产品
S2 采购按订单制造产品
S3 采购按订单设计产品
制造
M1 制造库存产品
M2 制造按订单制造产品
M3 制造按订单设计产品
交付
D1 交付库存产品
D2 交付按订单制造产品
D3 交付按订单设计产品
D4 交付零售产品
客户
采购返回
SR1 返回不合格产品
SR2 返回需要维修产品
SR3 返回多余产品
交付返回
DR1 返回不合格产品
DR2 返回需要维修产品
DR3 返回多余产品
使能　计划　采购　制造　传送　返回
1) 建立和管理规则
2) 评估性能
3) 管理数据
4) 管理存货清单
5) 管理固定资产
6) 管理运输
7) 管理供应链配置
8) 管理法规遵从
9) 管理具体元素
联合金融　供应商同意

图 4-4　SCOR 模型第二层流程[SCC2005]

第三层分解层(如图 4-5)：它给出第二层每个流程分类中流程元素的细节，为企业提供制定成功计划、设定完善供应链的目标以及提高供应链绩效所需要的信息。支持第二层的所有业务流程，每一个第二层流程由多个相应的第三层流程组成。

图 4-5 SCOR 模型第三层流程[SCC2005]

第四层：具体定义都是根据企业自身情况决定的，具有特殊性，所以没有在行业标准模式中定义特殊元素的可能性和必要性。在实施层中，各个企业根据自身供应链管理的实际将第三层中分解出的流程元素进行再分解，从而获得竞争优势并适应商业流程的变化。

SCOR 旨在实现供应链伙伴间的有效沟通。作为一个行业标准，通过解释流程间的

关系(如计划与获取,计划与制造),有利于推动供应链内外部的合作、水平流程的整合。它也可用作数据的输入,完成供应链类型选择方案的分析,如第二层,按库存制造(产品或服务根据预测生产或提供)还是按订单制造(产品或服务根据客户的实际订单生产或提供)。SCOR 用于描述、度量和评估供应链,支持战略规划与持续改进。

2. 度量指标[LHH2009]

SCOR 模型包含 150 多个关键指标度量供应链运作的绩效。与流程模拟系统一样,这些指标也按层次结构进行组织。绩效指标与绩效属性一起使用。绩效属性是指供应链的特征,它使得我们可以对它和其他使用竞争策略的供应链进行分析和评估。这一点就像你如果要描述一根木材,需要使用长、宽、高这样的标准特征,供应链也需要用标准特征来描述。否则,极难将一家选择低成本供应商的企业与一家选择可靠性高的企业进行比较。表 4-1 给出了绩效属性的例子。

表 4-1　SCOR 供应链风险管理功能模块与绩效属性[LHH2009]

	定　义	可选绩效属性			
		供应链可靠性	供应链响应性	供应链敏捷性	供应链成本
计划(P)	结合企业全面风险管理计划来识别、协调和管理供应链风险的过程	—	—	① 行业基准比较(%) ② 期权或套期保值率(%)	全面风险或风险事件化解成本($)
获得(S)	识别和评估可能影响企业或供应商以准确的时间、合理的成本和可接受的质量向用户交付物品的能力的采购风险	① 供应商风险化解计划的实施率(%) ② 产品或客户绩效的风险价值(VAR) ③ 供应商风险数据时间(月)	外部事件响应时间(平均天数)	内部事件响应时间(平均天数)	全面风险或风险事件化解成本($)
制造(M)	管理与准时、低成本、高质量生产产品有关的风险,以及计划与实施响应措施以应对制造风险	① 供应商风险化解计划的实施率(%) ② 风险值(制造) ③ 供应商或客户风险数据的时间(月)	外部事件响应时间(平均天数)	① 行业基准比较(%) ② 内部事件响应时间(平均天数)	全面风险或风险事件化解成本($)
交付(D)	管理可能影响企业以准时、合理的成本和质量递送产品的能力的过程	① 风险价值(交付) ② 产品或客户风险数据的时间(月)	外部事件响应时间(平均天数)	① 行业基准比较(%) ② 内部事件响应时间(平均天数)	全面风险或风险事件化解成本($)

第一层指标与绩效属性相关。根据第一层各指标计算值,就可以评估出企业在竞争市场中取得理想地位的程度如何。第一层指标是根据低层指标的计算得出的。低层指标的计算(如第二层)一般与较窄的流程子集有关。如“交付”绩效可以这样计算:按承诺日期,准时和完整交付的产品总数量。

3. 最佳实践[LHH2009]

供应链运作绩效被评估以及绩效差距被确定以后,下一个重要问题是确定采取什么样的行动来填补差距。为此,SCOR 提供了 430 多项可操作的实例,它们均来自 SCC 成员企业的实际经验。

SCOR 模型对"最佳实践"的定义是:为了对理想运作结果产生积极影响而使用的具有现时性、结构化、已证实且可重复特点的方法。其中:

(1) 现时性:不可以是新出现的也不可以是陈旧的。

(2) 结构化:已经明确规定了目的、范围、流程和程序。

(3) 已证实:在某一工作环境中已经证明并取得了成功。

(4) 可重复:已经在多种环境中得到证实。

(5) 方法:业务流程、实践、组织战略、实用技术、业务关系、业务模型以及信息和知识管理等被广泛使用的方法。

(6) 对理想运作结果产生积极影响:实践表明,在运作方面已经取得了与规定目标相关的改善,并且能够与关键的指标联系起来。影响应该用收获(速度的提高、受益和质量)或减少(资源浪费、成本、损失和退货等)来表示。

4.2.3 模型的应用

作为全球通信网络的互联网,ICT 给供应链带来了极大的益处:为供应链参与者提供通信的基础设施,为基于互联网的执行供应链业务流程的应用程序提供平台;为数字商品提供了新的分销渠道;为有效的电子采购形式(例如电子市场上的电子采购)提供平台;带动了新的合作方法(例如协作计划 CPFR);促使新的全球信息服务的产生(例如供应链的电子采购产品目录);使供应链成员的合作更加快捷和简便(例如供应链成员使用互联网进行日常的协作可以带来商业利益,可以降低库存水平和资产循环次数);支持(双向)客户交互;基于互联网的客户接口的实现可以使其进入新的市场;简化了供应链改进的实现(例如供应商管理库存)。所以,我们有必要加强 ICT 供应链风险管理的实施。

对供应链委员会的 SCOR 模型的研究和应用可以使 ICT 供应链风险管理更加成熟。1990 年,供应链群体以自愿的方式组成了利益集团,共同开发一致的治理方法、系统生命周期方法、流程集以及子流程的实践和度量方法。供应链运作参考模型被 800 个个体或公共组织用以理解和管理供应链,是应用最广泛的供应链管理框架。如今的 ICT 供应链经理和过去的生产供应链经理一样,对 SCOR 模型有相同程度的关注和兴趣。成熟的供应链工业应该把 ICT 供应链风险管理提上议事日程并加以重视,这将有助于加速达成共识和全面发展。SCOR 企业风险管理模块直接定义了能够填补供应链风险管理委员会列出的 ICT 供应链风险管理缺口并能加速其成熟的风险治理方法论。具体来说,SOCR 模型通过五个阶段方法来支持有效的 ICT 供应链风险管理(如表 4-2)。

表 4-2 SOCR 模型进行 ICT 供应链风险管理的五个阶段方法

阶段	名称	可 传 送 的	决　　定
开始	建立	组织支持 风险管理项目	谁是发起者
1	发现	供应链定义 供应链风险优先级 项目风险程序定义	程序包括什么
2	分析	积分卡 基准 竞争需求 客户服务需求	供应链承受风险的能力
3	评估	地理地图 威胁图表 风险评估	初始分析-风险在哪,有多大
4	减缓	减缓计划 水平 3、水平 4 的进程 最佳惯例分析	最终分析-如何消除或缓和风险
5	实现	机遇分析 减缓定义 部署组织 减缓和响应项目	实施减缓

将 SCOR 运用于 ICT 风险管理,需要设定合适的指标。当使用这些指标时,我们需要牢记两个基本事实:供应链性能是通过终端客户对其总体性能的认可度来测量的,因此供应链管理应该面向集成整体而不是独立流程简单组合的性能;对供应链业务和产品策略以及价值命题指标的选择是至关重要的。

将供应链风险管理嵌入到 SCOR 模型中,是 SCOR 模型发展过程中的一大进步。SCOR 对供应链风险管理的功能和度量指标需要在今后发展中不断完善。目前的 SCOR 供应链风险管理,包括以下 3 个阶段:风险识别(能够产生一个可能损害供应链绩效任何方面的潜在事件的清单)、风险评估(让管理者了解最大的风险可能在何处)、风险化解(确定风险是否能够控制或监控)。[LHH2009] SCOR 的应用范围很广:从订单输入到付款发票以及其中所有相互影响的用户;从供应商的供应商到用户的用户,包括服务领域的物流,所有物质材料的交易;从了解总体需求到满足每一个订单以及其中所有相互影响的市场。

SCOR 可以构造出内部和外部的供应链;显示现有供应链的配置,找出理想的供应链管理流程;通过语言和流程定义,可以更加有效地进行内部职能部门、供应商和分销商之间的评价和沟通;评价自己的供应链过程的绩效,并与行业内外其他企业供应链进行比较;用标杆法和最佳实践数据把企业的活动分成不同次序,量化制定流程改进的潜在效益,确定财务评价指标;软件产品用于供应链过程的路线图,和供应商一起找出软件产品的特征;对进程中的流程改进的测量,可以找出最有效的努力方向。

4.3 ICT供应链确保参考模型

4.3.1 模型的产生背景

为支持美国总统发布的国家网络安全综合计划(CNCI)及其保护国家网络设施的紧急任务,2009年6月,美国科学应用国际合作组织(SAIC)和马里兰大学史密斯商学院供应链管理中心联合发布了合作完成的题为《建立网络供应链确保参考模型》的研究报告[SAIC&SCMC2009],强调在网络供应链生命周期中进行安全保障。该研究试图通过在不断演进的网络领域中运用供应链保护措施,将网络安全领域和供应链风险管理领域进行有效融合。

报告描述了网络供应链生态系统,给出了生态系统中关键行动者的角色,然后定义了一个包括战略关系、组织结构、运行参数和应用范围的网络供应链安全确保模型;明确了以下三个主要问题:(1)当前的供应链管理措施将重点放在实体(物流)供应链上,从而使网络供应链非常脆弱;(2)迫切需要明确一种全局性的方法来克服网络安全中的瓶颈问题;(3)迫切需要高效的自我调节。这三个问题存在共同支持建立一个标准的网络供应链确保参考模型的需求。

该研究将端到端的供应链管理引入到了IT安全研究领域。研究人员在全球供应链发展的最佳实践经验基础上,为确保分布式的IT安全不受威胁,首次提出了一个综合模型——网络供应链安全确保模型。该模型建立在动态管理结构基础上,并对IT软件和硬件的特征做了充分考虑。模型很好地体现了供应链风险管理和信息安全这两门动态学科的融合,不但对关键行动者、关键过程和薄弱环节进行了定义,还指出了国际生产和维护链条中每个节点的战略性依存要素。该模型表现为由三个嵌套的环组成的过程系统,这三个环分别代表了计划和操作控制的不同层面,用以解决系统开发生命周期中的深度防御需求和网络供应链中的广度防御需求[SAIC&SCMC2009]。

4.3.2 模型的基本原理

1. 实体供应链与网络供应链

实体供应链是指促进商品流通的活动的总和。流通过程中,商品经生产和装配后从源头(原材料或零部件)流向众多仓库、配送中心并最终到达个人客户。这一过程通常通过零售商店实现,现在则越来越多地直接配送至个人住宅或商业所在地。实体供应链还包括因返工或保修而出现的产品回流。除了商品的实体流通之外,供应链还包括方便商品流通所需的数据传输和金融交易。越来越多的公司日益意识到供应链对其全面成功经营的重要性。然而,供应链十分复杂,包括供应商、采购商、生产商、仓库和运输管理者,还包括批发商、零售商和客户。它们作为供应链的独立组成部分,分别具有决定性功能,供应链上任何一个环节的崩溃或失败都将降低整个系统的效能[SAIC&SCMC2009]。

网络供应链是指包含于或使用网络基础设施的关键行动者的全部集合,包括终端用户、政策制定者、采购专家、系统集成商、网络提供者以及软件/硬件供应商。这些用户/供

应商之间通过组织和过程层互动来计划、构建、管理、维护和保护网络基础设施。与实体供应链相类似，网络供应链是一个端到端的过程。该过程始于软件开发商，其职责与实体供应链上的供应商类似。实体供应链上采购部门、生产和分发管理者的角色与网络供应链上的政策制定者和系统集成商、硬件/组件开发商、软件供应商的角色极其类似。实体供应链上的消费者与网络供应链上的操作者/终端用户相对等［SAIC&SCMC2009］。

2. 网络供应链生态系统

以下是该项目为了描述网络供应链生态系统而给出的三个关键定义。

(1) 网络基础设施(Cyber infrastructure)：共同构成重要的国家和企业基础设施骨干的大部分ICT系统(包括硬件、软件和公共/私人网络)。网络基础设施使美国国防部、国土安全部及其主要供应商等关键的政府或工业基地参与者能够实施不间断的行动［SAIC&SCMC2009］。

(2) 网络供应链(Cyber supply chain)：也叫ICT供应链，指包含于或使用网络基础设施的关键行动者的全部集合，包括终端用户、政策制定者、采购专家、系统集成商、网络提供者以及软件/硬件供应商。这些用户/供应商之间通过组织和过程互动来计划、构建、管理、维护和保护网络基础设施［SAIC&SCMC2009］。

(3) 网络供应链确保参考模型(Cyber Supply Chain Assurance Reference Model)：一个不仅定义关键行动者、关键过程和薄弱环节，而且明确了国际生产/维护链中各节点的战略性依存要素的模型［SAIC&SCMC2009］。

在实体供应链上，供应链管理者负责确保从供应商到消费者的整个过程的完整性，这一保证过程包括监测和评估供应链上每一行动者的输出质量。同理，在网络供应链上，供应链管理者需要执行对应的确保职责，下面将明确网络供应链生态系统中每一关键行动者的职责(如图4-6)。

政策制定者筹备经营内容、决定服务质量和供应商绩效监控标准；生态系统采购专家力争将联邦采购条例的变化写入采购合同中，以进一步确保安全；系统集成商扮演跨供应商产品和服务的第一层协调者的角色，力争统一第二层供应商的评估标准，并寻求更为安全的跨供应商交易和交流平台；软件开发商负责管理软件系统、代码完整性和内核评估，并努力筛选出人为或病毒威胁；硬件/组件开发商管理第二层供应商，保证产品质量，防范赝品进入系统；网络供应商为网络供应链上的行动者的数据、视频和声音通信提供带宽和连接，为应用/服务主机提供安全的企业级服务器网络；操作者/终端用户，例如情报专家，必须处于系统中的最高信任级别，有清晰的路径将命令信号传送至供应商，并预期得到供应链反馈回馈的及时响应［SAIC&SCMC2009］。

3. 网络安全的“职能筒仓(Functional Silos)”现象

“职能筒仓(Functional Silos)”现象指组织的功能单元以实现自身职能目标为中心，只制定有利于自身职能实现的政策，完全不考虑这种政策是否可能给更大范围的组织整体带来负面影响。各个功能单元就像一个个孤独伫立的筒仓，相互独立，没有联系，这种状态下制定出的政策显然效率降低，重复度高，易起冲突。

“职能筒仓”对网络安全构成巨大的威胁，当前网络供应链中“各自为战”的现象是网络安全确保的最大障碍。有人把全球性ICT供应链比作一场没有指挥者的交响乐。“如

果可以将供应链比作是一支管弦乐队，那么请想象这里有104名演奏者，却没有指挥者；只有极少的活页乐谱；演奏者之间没有音乐交流。在这种情况下，怎么能演奏出一场交响乐呢?”这些“职能筒仓”根深蒂固的原因在于产业日益增长的专业化趋势和不断缩小的领域焦点，例如软件、硬件和系统集成。每个专业领域都习惯于一定的思维和行为方式，其结果是，就像地质层一样，时间越长，这些方式就越难改变[SAIC&SCMC2009]。

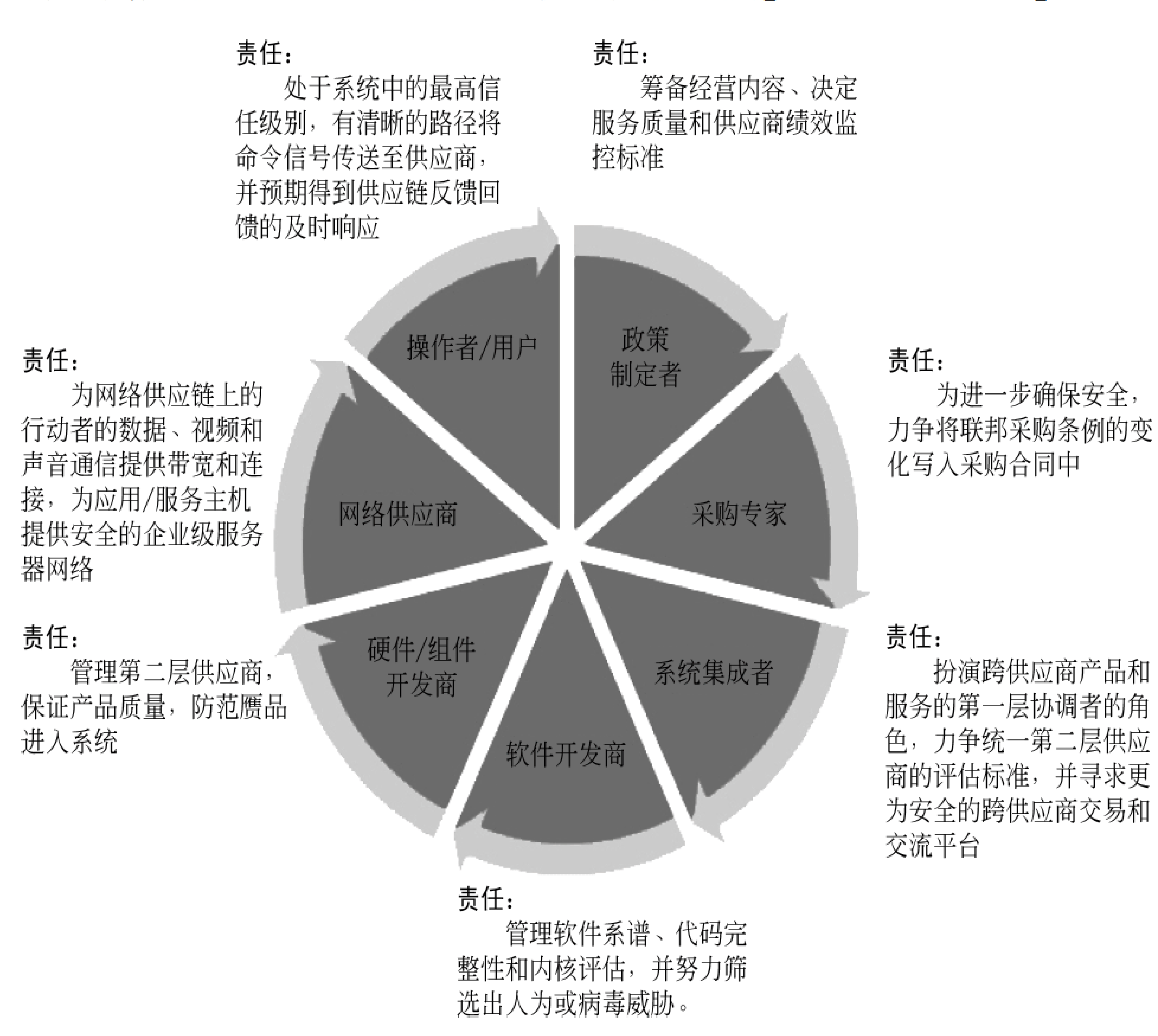
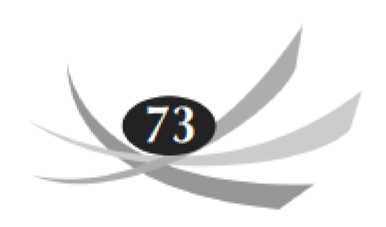


图 4-6　网络供应链生态系统[SAIC&SCMC2009]

网络供应链的强度有赖于供应链上系统开发生命周期内的相互信赖性。因此，经营策略必须在两个维度上展开(如图4-7)：垂直维度上，生态系统需要在系统开发生命周期内进行深度防御；水平维度上，生态系统需要在供应链上进行广度防御。这需要集成商将公共领域内供应商和消费者之间的共有风险经过揉合后再来实施风险管理。

在系统开发生命周期下方，多数组织关注那些符合用于建立一个易于理解的底线的既定政策、导向和措施的方法，整个系统的重点是管理变化控制/转移。然而，解决系统开发生命周期和供应链内的风险管理需要一个更为积极、持续升级的风险管理方法。这就使得用于调节每日商业变化和供应链关系动态性的实践方法成为必然。这种方法的目的是：建立底线并持续将主客观风险威胁降至可管理水平。

供应链上的广度防御节点不是绝对有利于供应链上制造和传送的产品、解决方案和服务安全。出现这种情况的原因是，网络供应链上的组织将自己视为终点而非轴心点或协调者。这种观点就会导致类似“在供应链中只关注对上保证供应商而不关注对下保证用户”的行为。这种单向的关注损害了组织的用户和用户的用户在供应链中的利益。意



识到这一点对网络供应链管理十分关键，因为与实体供应链不同，网络系统肩负着用单一解决方案服务多种类型的下游客户的任务（往往在多种具有竞争性的需求驱动下）。这种任务只有通过先进的计算行为才能完成，例如多任务、网络中心操作、云计算和网格计算等[SAIC&SCMC2009]。

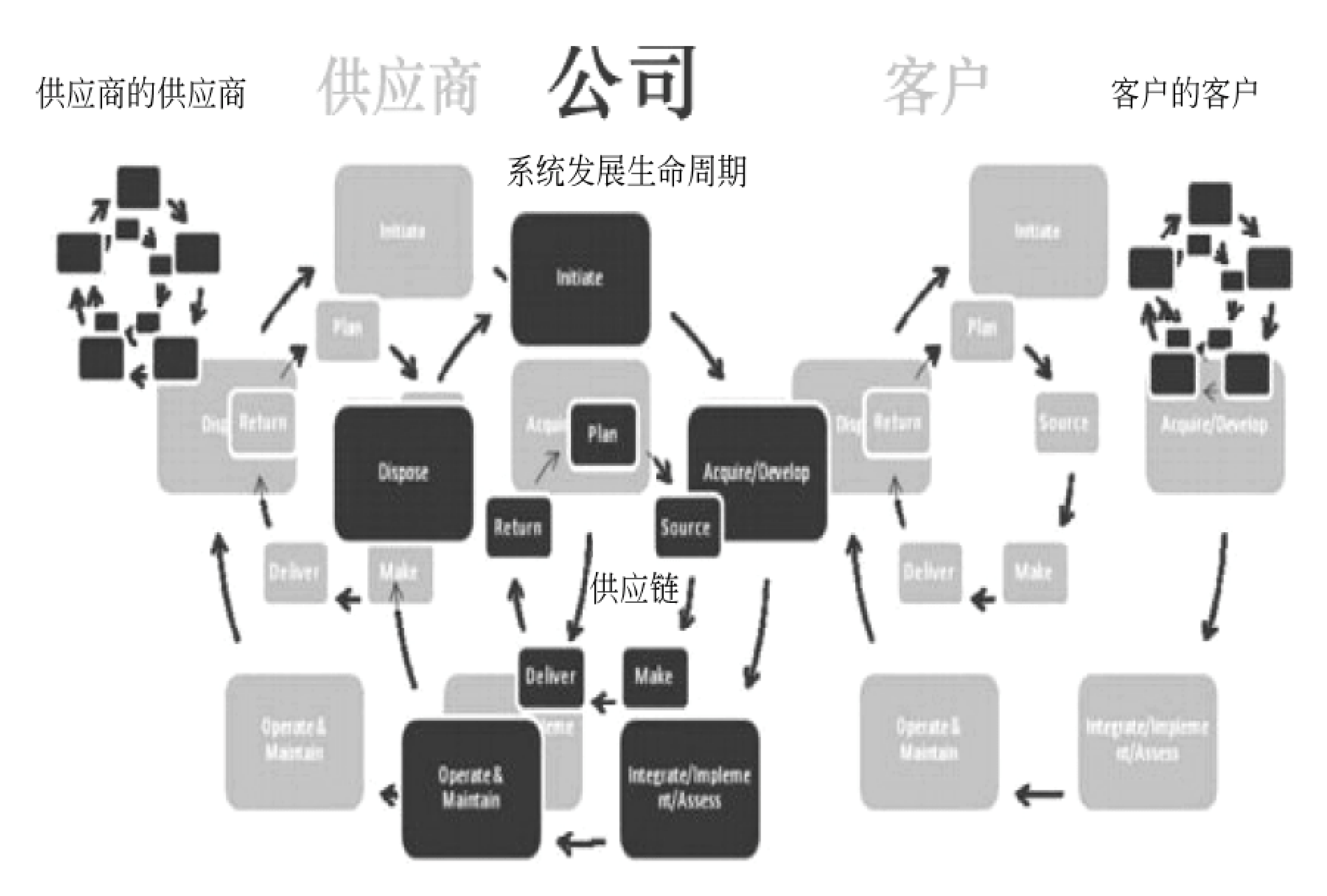


图4-7　网络供应链的两个维度[SAIC and SCMC 2009 P15]

“应用于”(apply to)和“全过程应用”(apply through)两个概念对于理解供应链上各系统开发生命周期中的相关性十分关键，它们推动了共有风险管理的渐近式发展。“应用于”安全投入影响供应链本身的人员、进程和技术，“全过程应用”安全投入则直接影响供应链生产和传输的组件、产品、服务和集成系统。图4-8展示了以三个关键阶段为重点的典型映射关系图，并将其扩展成为一个包括了相关行动者节点的典型生态系统，这三个关

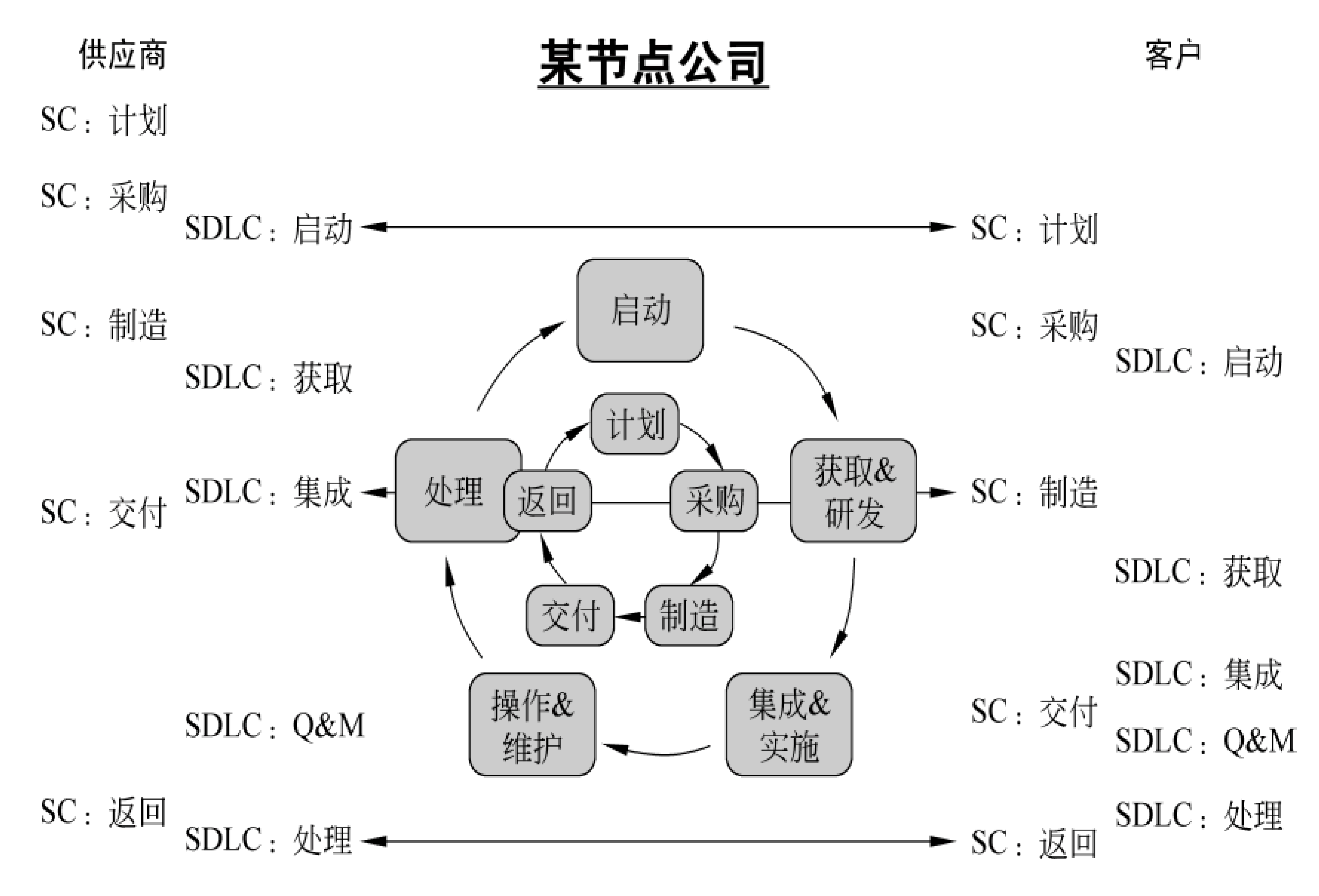


图4-8　单个节点的系统开发生命周期与供应链生态系统映射[SAIC&SCMC2009]

键阶段在各节点/行动者的系统开发生命周期和供应链之间的交集中实现同步。这些交集的定义和映射关系以及它们之间的相关性使供应链上的节点能够更好地控制共有风险。需要注意的是单个行动者的系统开发生命周期内的深度防御并不绝对地有助于其他行动者的共有风险管理[SAIC&SCMC2009]。

意识到将深度防御和广度防御进行有效连接的需求，推动了参考模型支持生态系统内各节点的系统开发生命周期和供应链之间的相互映射。这就意味着，从风险管理的角度对生态系统进行综合评估，供应链的协调者必须对供应链及其全过程实施安全缓解策略。图4-9描述了风险管理功能如何在技术堆栈中向上移动。初始焦点是面向产品构建模块，例如操作系统、应用程序和网络。随着复杂程度的加大，则必须构建平台和框架以支持周边产品供应商。最后，随着风险管理从单纯地关注技术功能驱动下的安全需求转向关注广泛商业目标驱动下的整体途径，模式最终实现转换。简而言之，这种更为广泛的战略远景支持端到端的商业模型。

随着系统或供应链的发展和壮大，网络市场焦点由适应性和分析向综合转变，风险管理可以在技术堆栈中向上移动(如图4-10)。在动态环境中降低风险不仅仅依赖于技术性缓解措施，它还要求在合同、经济、金融和政策中包含和反映一种深层次的“有条纹的”商业环境。当某一组织在技术堆栈中向上移动——从操作系统向完整的、扩展的企业级供应链管理移动，与用来解决风险管理过程中的问题(起因于威胁、薄弱环节、开发某组件或企业的影响)的传统分析方法几乎没有相关性，它将重点转移至系统思维和系统综合，从而研究供应链生态系统元素之间的内在关系和相互信赖性。最后，各组织都将注意力集中于供应链上系统开发生命周期之内在关系的处理上。

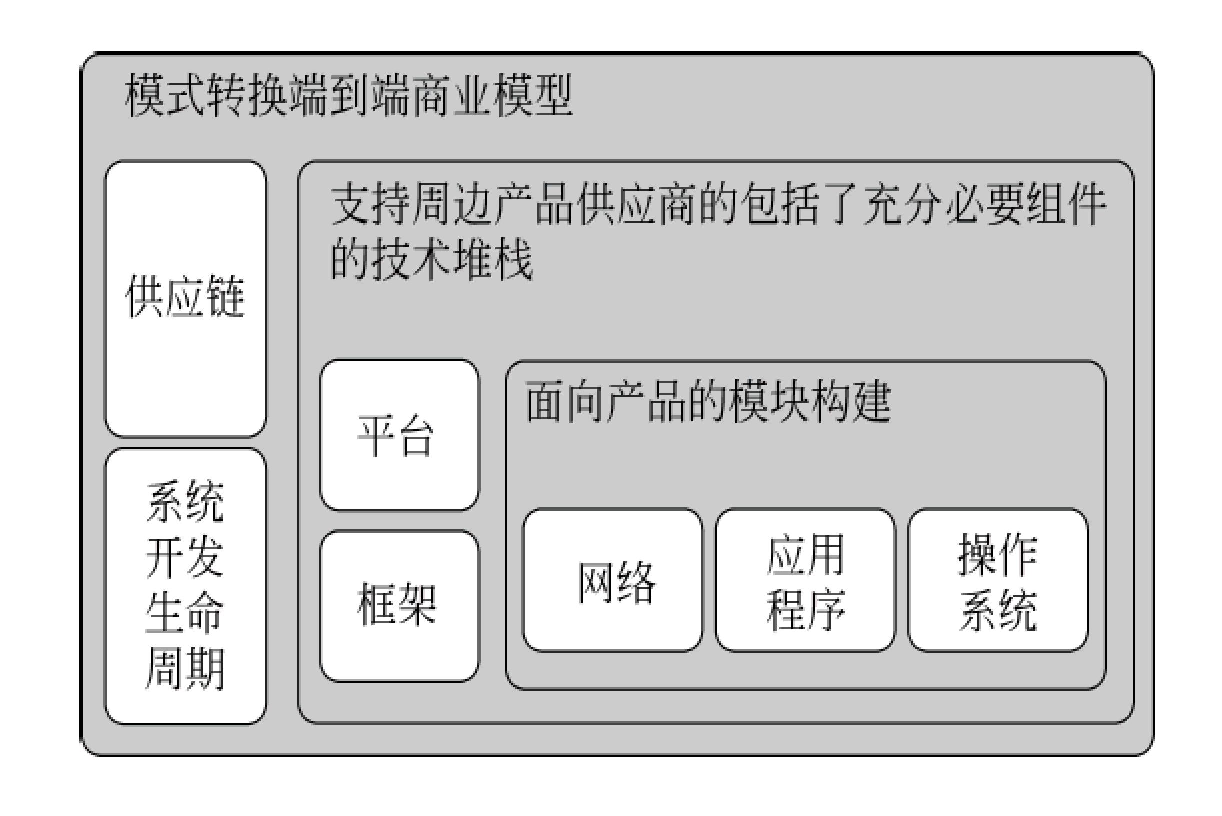


图4-9 端对端商业模型模式转变[SAIC&SCMC2009]

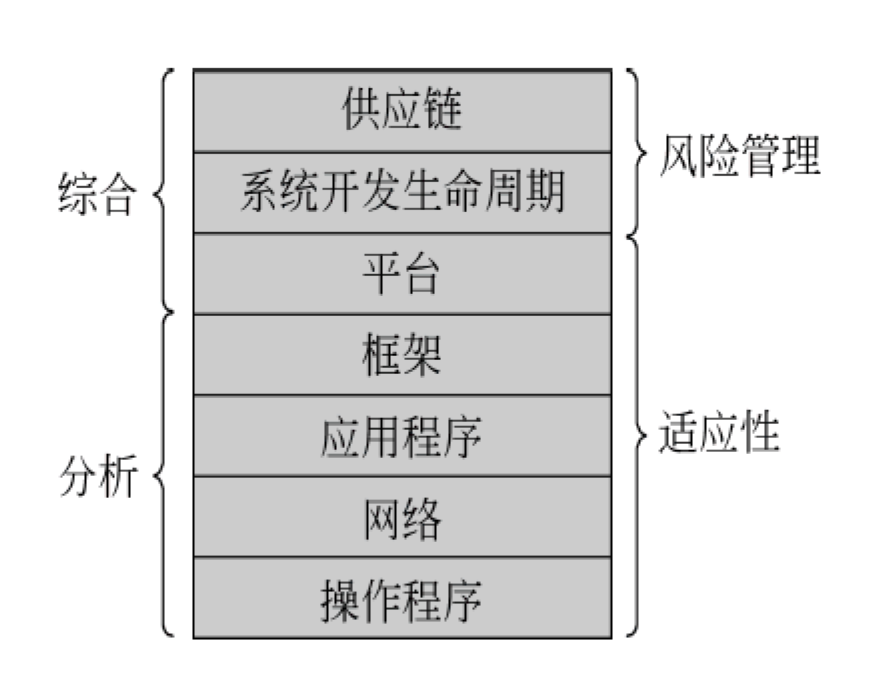


图4-10 风险管理在技术堆栈中向上移动[SAIC&SCMC2009]

4. 网络供应链确保参考模型

在给出网络生态系统的基础上，可以给出网络供应链确保参考模型。ICT供应链安全确保模型最重要的目标是：明确一系列相关原则/措施及其组织框架，如果这些原则/措施得以有效实施，合作机构的构建、运营，ICT供应链系统的整体性和质量以及高度集成控制的实施将成为现实。此模型从行动者的共同利益出发，不仅使其对上负责，更要对整个供应链负责，在转变中将合作关系嵌入其中。该模型表现为由三个嵌套的环组成的过程系统，如图4-11所示。这三个环分别代表了计划和操作控制的不同层面，用于解决

系统开发生命周期中的深度防御需求和网络供应链中的广度防御需求，分别为：

管理环节（环1）：该层面解决的需求包括指令的统一；数字供应链战略规划和风险管理的一致；有效的网络设计和配套规则的发展；业务生态系统关系的正常化；最优化政策的推行等。该环节主要解决ICT供应链安全风险管理相关问题，明确网络供应链风险管理需求和客户是"集线器"组织的驱动力，客户代表着管理功能——集线器的核心环。

系统集成与共享服务环节（环2）：这一层面解决的需求包括严格的功能整合；网络供应链实时可视/监视系统的发展；连续的监察审查管理；确保连续的监管/系统质量高度积极的干预措施；操作的连续性等。该环节主要解决ICT供应链中运维服务的安全问题。系统集成商代表网络供应链的指挥功能，是距离中心第二近的环，目标是说明客户需求，其角色是"集线器"的服务"手臂"，是实现高度同步的委任、设计、构建、保持和处理活动的"指挥家"。

行动与实践环节（环3）：这一层面解决的需求主要包括特定行动角色的最佳实践过程和综合的网络/有形资产管理，同时包括受强烈的全球化ICT供应链风险威胁的组织目前正在使用的基准措施的定义、收集和分发。该环节主要解决ICT供应链自身的安全问题，或者说解决ICT产品生产制造中的安全问题，包括软件供应链和硬件供应链安全问题。网络供应商代表部署功能和行动环（最外的环）。他们提供软件、硬件、网络产品和服务，是核心系统的组成部分。供应商环围绕着整个环结构，管理着广泛的实体设备、工作场所和虚拟知识产权。

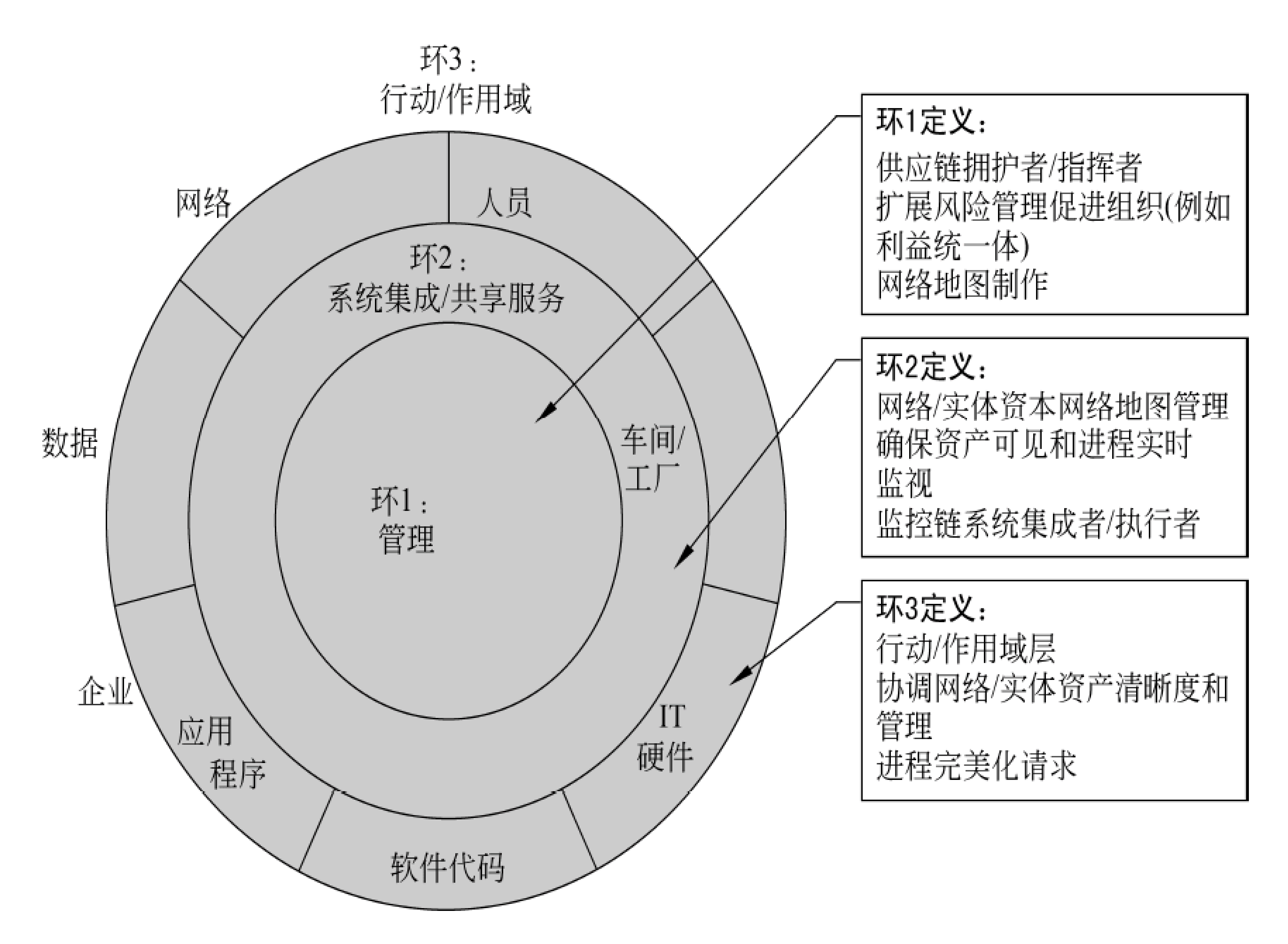


图4-11　ICT供应链安全确保模型［SAIC&SCMC2009］

这里非常明确地预设模型的管理功能，并不是应该由一名供应链"沙皇"自上而下以集中管理所有的战略和战术行动，这种模式在网络世界中根本不可行。相反，本模型推崇一种"管理"模型，在共同利益宽松联结的基础上实现灵活一致。将有越来越多的这种利益共同发挥作用，设计虚拟的网络供应链，定义其或松或紧的内部联结结构用以集中管理

ICT 供应链。因此，可以将模型相互嵌套的环作为虚拟综合和内在关联性的比喻，它们对实现 ICT 供应链的有效控制是至关重要的[SAIC&SCMC2009]。

模型面临的最大挑战是雇佣呈散布状态的行动者，这些行动者有自己的专属商业领域和任务，但总体的任务均是保护 ICT 供应链的安全。这些专注于各自事务的行动者必须将目标迅速转向构建集成供应链的艰巨任务中。“相互敌对的部分”必须学会结成联盟并在服从统一指挥的条件下为生存而斗争。要实现以上预想，必须使利益统一体中的成员形成联合文件，概述共同的确保愿景，分析和明确供应链中的核心风险，并对这些分析进行优先级排序。模型的综合功能并不一定必须由独立机构或专有的系统集成公司完成，而是可以由专有的内部网络资源来完成[SAIC&SCMC2009]。

每个环或每类人员有其自身的利益和动机，其自身的商业或运营动力促使其在端到端供应链中属于自己的那部分寻求更高的透明度。目前尤其特别的是，在全球经济和政治不稳定的严重形式下，每类人员都试图对当前的不稳定因素施加战略性的影响。参与这个项目研究的人员能够代表来自公共和私有部门的顶级网络安全专家。根据广泛的背景研究和与这些顶级思想专家的 30 场访谈，这里收集了一系列具有代表性的各个环的最优措施(如表 4-3 所示)[SAIC&SCMC2009]。

表 4-3　网络生态系统各个环的最优措施[SAIC&SCMC2009]

环 1	• 明确指挥和控制/明确供应链指挥者，监控行动者和整个过程效率度量之间的端到端流通和传送； • 建立由链上关键部门的代表(包括政府部门，例如利益统一体)组成的扩展企业风险行动小组； • 建立网络地图，将位置上散布的网络供应链产品/发布/消费“集线器”网络节点以及“集线器”和节点之间的流通/传送可视化； • 审查和模拟整个链上分布的风险；对缓解行动进行风险优先级排序；将优先分队分配至所有者，将资源分配至风险拥有者； • 制定联合风险行动文件，作为从各部门到项目发起者的保证声明和证明； • 明确网络供应链保证关键战略/战术标准，并嵌入组织座舱控制和仪表显示； • 致力于完美采购：仔细检查供应商历史，只使用风险特征被检查过的软件； • 坚持风险缓解措施/第一层供应商向第二、三过渡的可追溯的条款； • 主要签约人应确保客户(政府或企业)了解向下的变化，为客户提供拒绝的第一权利/没有优先者的同意不能允许合同转包； • 努力通过市场压力增加粗心的供应商的“成本承受”责任； • 通过战略财政审查/风险分析提升公司的健康程度和风险等级
环 2	• 创造和管理风险登记，捕捉/明确网络供应链优先风险、风险拥有者和持续的缓解措施； • 追踪仪表盘度量：实时关键业绩指标，主要和次要的指标； • 重点关注正式 & 全面的网络供应链资产管理方式； • 通过散布的网络站点，构建全球清晰度网格，一种集中管理的“指挥所”，配置和监控数字 CCTV 和自动接入控制，以实现威胁定义和实时缓解； • 合理考虑供应基地，把重点放在信任的供应商上； • 分离/设置核心供应商的运营/设施地图； • 可见/向下追踪次级供应商；

续表

<table>
<tr><td>环 2</td><td colspan="2">• 实施电子档案/监控文件链，建立简单的、可被链上所有人员运用的在线系统开发交互记录；
• 将保证措施和承诺条款写入供应商合同，构建供应商“自责任”和保证证明；
• 实施运程站点持续审计/监控方法，例如：供应商站点代码扫描引擎是过程中的监控工作，如果供应商将其关闭，合同将立即终止；
• 减少/简化组件/技术传播，以实现更好的标准/控制；
• 海外在软件进入本国境内的网络前接受相关测试，这一条款应写入合同；直到客户接受测试结果之前，相关费用应被扣留；
• 以开发服务器、筹备服务器和产品服务器为基础，严格实施有步骤、有门槛的接收程序；
• 对有安全先例的系统新组件(非旧组件)实施增值审计；
• “清理船只”：在将服务器、个人电脑和笔记本电脑移到其他用户站点时，采购、组装、装载、装备、配置和锁定程序进行集中化处理；
• 从硬件驱动向自动无盘工作站、企业级服务器应用程序/数据和软件远程升级过渡</td></tr>
<tr><td rowspan="4">环 3</td><td>网络</td><td>• 多法并举进行网络脆弱性演练；
• 技术性突破团队应力测试；
• 恢复“参考监控观念”：如果侵入系统在持续工作，就停止运转；
• 侵入检测系统；
• 降低“挥动的比特”：为实现更好的控制和保证，将云计算设备集中到最近的终端用户群；
• 以分类或敏感网络，实施“空隙”——网络之间不用物理/铜线连接，或者只使用光纤设施；
• 基于属性访问/全球轻量级目录访问协议任务/许可；
• 在网络内部严格实施“信任区域”；
• 带访问控制日志的数字 CCTV 集成 & 用于监控网络威胁的轻量级目录访问协议任务/许可；
• 建立“诱饵系统”：位于脆弱区域(例如虚拟机上未保护的浏览器)的机器，用于索引感染，诱使侵入者“伸手”；
• 数据丢失保护/数据渗出</td></tr>
<tr><td>数据</td><td>• 把重点放在新的高德纳魔力象限领域：运用企业应用程序安全以保护员工和客户的关键数据；
• 确保与美国、欧洲的相关个人数据和机密条例相符合；
• 对数据进行足够安全级别的加密；
• 为数据访问提供技术或其他鉴定机制；
• 主服务器保持时间敏感数据；
• 为更为敏感的数据提供高保证级别的路由器</td></tr>
<tr><td>企业应用程序</td><td>• 实施关键分析/风险评估；
• 为实现全球一致性管理，确保所有参与者与企业轻量级目录访问协议一致；
• 确保应用程序供应商对内部 IT 员工进行关于应用程序安全最优措施的培训</td></tr>
<tr><td>软件代码</td><td>• 内部风险行动小组与产品小组共同努力，提升安全开发生命周期意识/整体性；
• 强调“三位一体”安全：编译、内核和虚拟机；</td></tr>
</table>

续表

环 3	软件代码	• 内部代码质量审核小组在混合代码提供过程中分离和评估第三方代码； • 自动代码脆弱性分析； • 代码数字签名； • 过滤代码/将代码限定至公司/组织防火墙外的代理服务器仓库，直到获取“健康报告”； • 安全代码仓库只接收预检验代码； • 用共享配置管理系统实现加强软件供应链安全属性/档案/监控需求链； • 改善新兴的有选择病毒清除技术，使管理层能够找到感染文件，而非像当前那样，将机器重建至未感染状态； • 在刻录软件 CD 或向客户分发前，使用正式进程标准来实施质量/安全检测（例如病毒扫描等）； • “信任区”限制性访问监控
	IT 硬件	• 合理化供应基地/将重点放至信任的供应商； • 进行经常性供应商在线审查（包括突然检查），把与供应商一起听取审查报作为一种持续开发创举； • 根据安全保证认证受信任的代工厂：对员工和访问者进行前门扫描，人力资源部门提供员工/合同工/供应商实时名单
	车间/工厂	• 通过阻拦/报警系统扩展安全视界； • 对所有访问者进行前门扫描； • 通过焦点监控/严格访问控制构建/执行“信任区”； • 努力将本地 CCTV 和访问控制系统连接至本部网络指挥所，以实现远程监控/反馈； • 在允许供应商工厂直接将产品传送至终端用户前，对其进行认证
	人员	• 通过信用/背景审查对所有竞标人/供应商进行排位； • 对所有供应商进行预产品审查； • 对关键人员实施预先雇佣审核措施； • 确保人力资源部门提供 IT 部门的实时员工收入和工作情况，以保持 LDAP 的实效性； • 通过内部人力资源或第三方培训者，开发安全软件生命周期措施的正规证书/认证； • 对不满的员工保持警惕，因为他们有可能成为重大的内部威胁

4.3.3 模型展望

20 世纪 90 年代早期，史密斯商学院供应链管理小组对数百家正在实施全球供应链转型的公司进行了研究。他们指出，当今网络供应链管理者与 20 世纪 90 年代的实体供应链的管理者在努力获取运营的清晰度、建立世界范围内协作性更强、更健康的客户、经销商和供应商生态系统方面做出的努力，有极大的相似性。20 世纪 90 年代早期，全球供应链管理者应对供应链分散挑战的方法是制作过程图并设定系统的行动准则，以应对运营中的复杂情况。从这些过程图和行动准则中，管理者开始构建更为有效的实体供应链。我们需要借助网络供应链确保参考模型，围绕 ICT 供应链的定义和目标达成一系列共识，这种 ICT 供应链必须能够满足下列测试［SAIC&SCMC2009］：

(1) 实现“深度防御”(系统开发生命周期)和“广度防御”(供应链)。

(2) 提供网络供应链清晰度和连贯性,实现有效的组织和协调。

(3) 在组织结构方面采取激励措施,促成合作关系,从而鼓励和促成共同风险管理。

(4) 改进网络和实体供应链之间的沟通。尽管网络和实体供应链有许多类似的用途和终极目标,但这两个领域之间交流的缺失,将会限制其发展。

(5) “应用于”和“全过程应用”对于理解系统开发生命周期和供应链之间的内在联系十分关键,也推动了共有风险管理的方式变革。“应用于”投入影响体现供应链本身的人员、过程和技术。“全过程应用”投入则直接影响供应链生产和传递的组件、产品、服务和一体化系统。两者对基于系统开发生命周期和供应链之间的内在联系来开发正确的解决方案来说,是十分关键的推动因素。

下一步的任务是进一步验证网络供应链确保参考模型,努力以该模型为依据开发一种评估工具,并根据最优措施的接受情况分析结果、区分反馈。把这些反馈用于开发改进型ICT供应链成熟模型。这些研究将以实际作业为依据,并努力将此模型有选择地应用于多国公司和政府机构并进行实证研究。将对以下内容进行进一步探索:

(1) 与环1的客户合作,组建网络供应链利益统一体,准备模型许可证书,实施风险定义/管理实践。

(2) 与环2的系统集成商合作,根据统一体的缓解优先级构建风险登记原型,并在备用网络供应链上设计监控系统链。

(3) 与环3的供应商合作,为可行的监控系统链开发过程承诺标准,并将智能光网络连接到该监控系统链。

随着对该模型改进研究的进一步发展,应开发更大的组织项目并构建更为综合的ICT供应链,努力与更多的标准开发组织合作,为更加严密的网络供应链确保标准奠定基础[SAIC&SCMC2009]。

4.4 供应链安全维度模型

供应链安全维度模型是在普华永道(www.pwc.com)于2011年底发布的《运输和物流2030卷四》[TLSSC2011]中提出的,目的是为了应对全球化背景下的供应链安全问题。它根据关键绩效指标法(KPI)和可以开展行动的时间范围,从五个方面对供应链安全进行了综合考虑[TLSSC 2011]。

4.4.1 模型的产生背景

能力管理、成本控制和现金管理这些词语代表了运输和物流运营商在当前的经济环境中面临的一些挑战。对于每家公司来说,为了解决危机,迅速而坚决地采取行动是至关重要的;对于一些公司来说,适宜地做出反应关乎生存问题。企业领导人不应忽视市场中的长期趋势,应该确保对其组织的可持续发展进行合理定位。《物流和运输2030》是解决这些问题的一系列出版物,它由普华永道和物流行业成员编写,并获得了欧洲商学院供应

链管理学院专家的大力协助，通过对全球20多个国家的多名专家进行德尔菲调查，高瞻远瞩地展望到2030年前行业的发展趋势。出版《运输和物流2030》的目的并非预测未来，《运输和物流2030》旨在成为精神食粮，成为行业领导人、战略专家和其他主题专家深入讨论中的“刺激方案”。

看起来2030年还很远，这个时限有点超乎人们的想象，《物流与运输》计划设想一直到2030年，看起来预期有些过高，但研究人员还是从中得到了一些强烈的共识，即人们都认为商业领袖和政府要关注长期的、以情景设定为基础的思路和规划。基于第一卷所引起的共鸣，普华永道撰写了一系列的预测报告，具体如下［TLSSC2011］：

油价长期以来都是运输和物流的关键因素。但是在过去的两年中价格剧烈波动，人们逐渐认识到能源在运输中的重要性，因此行业比以往更迫切地需要开发前瞻性的解决方案。《物流与运输2030（卷一）》于2009年10月出版，特别关注了能源的稀缺性及其对行业的影响。

港口、机场、公路、铁路、桥梁、隧道，这些设施都具有相同的特点，即使使用寿命不到几百年，也能达到好几十年，这需要对运输基础设施的需求及其对经济和环境的影响进行长期预测，对建设、运作和维护的财政需求也要进行长期规划。运输基础设施如何跟上不断增加的货运量要求，应当本着满足快速、高效、可靠并使环境可持续性发展的这一持续增长的要求制定运输解决方案。《物流与运输2030（卷二）》特别关注了运输基础设施的长期规划问题。

几乎在全球每个角落都能享受到物流服务，如果仔细观察，我们会发现这些物流服务存在明显差异，全球的物流公司在以后几年和几十年里还会面临各种挑战。新兴市场会发挥主要作用，但这些国家的交通和物流行业在二十年后发生什么变化？物流中心会向东移动，还是向南移动？全球运输网络会出现什么新的运输枢纽？谁将成为新兴市场的领导人？《物流与运输2030（卷三）》特别关注了未来新兴市场是否能成为新的枢纽中心或新的行业领导。

不论是出于政治还是纯粹的利益原因，货运和客运设施经常受到攻击。毁灭性地震和自然灾害（如日本海啸）使人们看到了当今的运输和物流系统的脆弱，例如，重要商业港口无法使用；更不用提这些事故给人类造成巨大伤痛。随着电子数据交换在相互交叉的价值链中发挥着越发重要的作用，对数据安全和工业间谍的忧虑也提上议事日程。普华永道于2011年底发布的《运输和物流2030（卷四）》［TLSSC2011］，对全球化背景下的供应链安全进行了阐述，报告着重指出了ICT供应链面临的安全威胁，有三个主要的发现：

（1）对供应链的人为攻击呈现上升趋势，运输和物流公司在选择运输路线时，需要将安全因素考虑在内。

（2）投入巨资保障ICT系统免于遭到网络攻击应该成为强制性的措施。

（3）没有供应链是100%安全的，更好的技术和经过良好培训的人员可以极大提高供应链安全。

4.4.2 实时德尔菲技术

传统的德尔菲技术是由美国RAND公司于20世纪50年代为了克服如从众效应、失

败效应和光圈效应等一般团体的效率低下问题，为统一专家对关于未来发展趋势的意见而系统开发的。通常的德尔菲预测流程以匿名、书面、多阶段调查流程的方式进行，每一轮之后对团队的意见进行反馈。普华永道将德尔菲研究设计为一种以互联网为基础，几乎是实时调查的形式，它通过使传统流程更为合理化以及使整个过程更具趣味性来为所调查专家提供更为舒适的环境，从而提高预测的有效性。采用这种技术，大部分的数据结果分析还可以实现自动化［TLSSC2011］。

根据大量的桌面研究、专家咨询和研讨会讨论，普华永道和供应链管理研究所为2030年的运输和物流业列出了18种关键的德尔菲预测，主要集中在能源效率和供应链速度方面。请所邀请的专家对这些论题的发生可能性(0～100%)、发生后对交通运输和物流业的影响(李克特5分评分法)和期望(李克特5分评分法)进行了评价并说明(可选)所有答复的原因。第一轮之后，给出对某项预测的答复，并立即计算所有参与者的团体意见并显示在了第二轮的屏幕上［TLSSC2011］。

专家们还可以读取其他专家为预测所提供的支持性论证。根据这种资料，可对第一次评估进行重新评价和调整。完成问卷表之后，各专家可在任何时候通过其个人邀请链接返回德尔菲研究的入口处。而后引导他们到“一致意见入口”处，再次可以对正在进行的德尔菲流程进行监控并可以单独地进入每项论题的评价屏来对自己答复进行修订。实时德尔菲调查的最终结果构成了机遇和中断分析的框架。根据大量的定量调查数据和案头研究，在接下来的专家研讨会中进一步地阐述这些预见认知［TLSSC2011］。

德尔菲研究的目的并不像大部分传统的调查一样是为了得到某一样本人群中的代表性意见。德尔菲研究的目的是为了融入更多的专家意见。承担此次德尔菲专题研究的团队由著名的全球型公司高级管理层代表、战略专家以及物流领域业务协会和学会的专家组成。主要的选择标准是行业和教育背景、工作经历以及在组织内外的职能。参加者来自各大洲的20个不同的国家，保证了对未来看法的均衡和全球性。为了使团队更有差异化和多样化，团队小组还包括了学术认知、政治家以及行业从业者，其中从业者占大部分。

4.4.3　对2030年的预测

未来会看到越来越多的对供应链和物流枢纽的攻击吗？网络攻击在运输和物流上会引发巨大破坏吗？哪些是保障安全的重要方式——是高科技还是安全审查还是其他？这些措施会大幅增加运输成本并降低运输效率吗？目前，各个国家都处于长期虚拟攻击的影响下，每两秒钟，德国互联网就会被攻击一次。作为全球化的发动机，物流会在未来成为犯罪分子的攻击焦点。例如，黑客会侵入飞行控制系统，并随意让飞机从空中掉落，或干扰路轨系统以致列车相撞，那时候我们该怎么办？网络攻击引发的有形损失将是运输和物流业越来越大的威胁。以下列举了德尔菲实验中专家组对未来供应链安全问题的相关预测及分析，这里着重介绍网络攻击方面的预测［TLSSC2011］。

(1) 供应链上的攻击数量将会增加。并不是所有专家组的专家都认同未来攻击的数量将大幅增加的可能性，他们分成了两个不同的阵营：一个组(忧虑专家，60%的样本)相信未来供应链攻击的数量将会大幅增加；另一个组(放松专家，40%的样本数量)没有预见未来供应链攻击的数量大幅增加。不管是忧虑组专家或是放松组专家，大部分的专家都

不希望攻击数量有大的跳跃。而有些专家反而乐见攻击数量的上升，他们认为这些攻击将会让相关组织把找出解决方案和开发更为安全的供应链作为首要事务处理。各个组织将更有动力执行他们的安全措施。

（2）网络攻击将可能导致比物理攻击更大的破坏。在《运输和物流 2030（卷二）》中，信息通讯技术（ICT）领域的一系列创新将有可能使交通基础设施的容量和使用率达到最大，供应链越来越依赖信息通讯技术。随着高速公路和公共交通的流量控制系统的安装的实现，网络攻击可能造成的潜在破坏也将变得更为严重。跟踪、检查系统的频繁使用和带有网络接口的实时控制的应用，为网络犯罪提供了越来越多的脆弱点。网络攻击对供应链造成越来越多的威胁促使很多高科技供应商共同合作，制定对抗网络犯罪的策略。波音、思科、IBM、微软、NASA 和美国国防部正一起努力研发可被国际接受的框架来保障供应链安全，防止网络攻击。新的标准将有助于避免网络犯罪分子在设备通过供应链时把安全漏洞引入到 IT 设备中。企业需要增加在安全项目和安全人员上的投资来保障技术，防止网络攻击，降低大型事故发生的风险。

（3）破坏和行业间谍将影响供应链，但是竞争者将不会是主要的攻击来源。破坏和行业间谍将会不是运输和物流行业中的一个问题，行业间谍的典型受害者是创新研究和发展比价格或者效率更为重要的行业中的企业。比如在汽车行业或者制药行业的技术领先者们，需要保护他们的产品和产品技术以及其他形式的知识和创新，以防止竞争者的攻击。此类事故在运输和物流行业中还是比较少见。除非物流运营商增加创新的投入，这种情况才可能发生改变。所以破坏和行业间谍不是运输和物流企业的主要担心。

（4）为了获得更高的安全级别，对数据隐私的担忧正不断被忽视。德尔菲专家组预见“隐私”的定义将变得更松散，尤其是在人们更为忧虑的地方。虽然很多人更愿意保持数据的隐私，但也准备好在需要时牺牲数据隐私，比如防止恐怖袭击。对于个人，数据隐私是个人问题。但是在供应链管理上，这个问题更多的是涉及商业实体间的关系，而不是个人的数据。一些专家担忧，公众们遇到安全措施的负面影响时，比如永久的监视，会对隐私问题产生忧虑。专家们认为新技术系统将既能保证数据的机密性，同时又不会阻碍安全和贸易。

（5）处理危机的策略比预防措施对处理供应链威胁更加有效？专家组的回答是——绝对不可能。仅仅对危机情况做出反应是不够的。各个组织需要采取预防措施来减轻安全风险。一些专家们指出供应链一旦被破坏，付出的代价是巨大的，也是不可预测的，影响可能会持续很长时间。比如，墨西哥海湾的漏油清理和补偿措施花费了数十亿美元。他们认为预防措施，包括潜在危机的减轻计划需要尽早就位。前期措施可以带来具有更好导向的政策决定和服务供应。在前期措施上的投资有助于降低公司的保险费率。很多专家注意到前期措施和预防解决方案不能被分开处理。安全策略通常来说都将预防措施和反应措施相结合。供应链是复杂的，一些运输和物流运营商在世界范围内的多个领域内运营，使得单纯的一个预防方法的实施变得十分昂贵，企业们必须找到预防和反应措施的正确结合，使供应链确保达到最优水平。

（6）到 2030 年技术是最好的保障安全的方式。“忧虑”专家组认为技术是最好的解

决方案，是供应链安全管理的前进方向。有些人更愿意用电子监控设备、“防黑客”系统和其他覆盖面较广的技术，取代人员密集的解决方案。这组专家认为，一直以来供应链中最薄弱的环节是人员因素，未来也是。他们的解决方案是尽可能用技术设备替代安全人员。没有供应链永远是100%安全的。技术可以帮助提高安全性，但人员是关键的一环。“放松”专家组认为即使是目前最先进的技术和设备，也不能完全成功地防止供应链攻击发生，未来趋势是技术，训练有素的人员和政策的组合。

虽然专家在有些问题上有分歧，但是全球供应链和运输风险已成为当今世界发展不可回避的问题，以上假设让我们不得不提高警惕，做好防范措施，下面将给出供应链安全维度模型并给出应对风险的有效措施。

4.4.4　模型的基本原理

如何优化自身安全配置来应对预测的未来威胁？如何进行强度测试并提高自身供应链安全性？根据关键绩效指标法（KPI）和可以开展行动的时间范围，在本节对供应链安全的五个方面进行了综合考虑：人员安全、信息和通信技术安全、过程安全、物理安全、供应链的安全伙伴关系，并为每个方面提供了考虑到主要运营指标（KPI）及执行时间的建议执行计划，这里我们将其总结为供应链安全维度模型（如图4-12所示）。

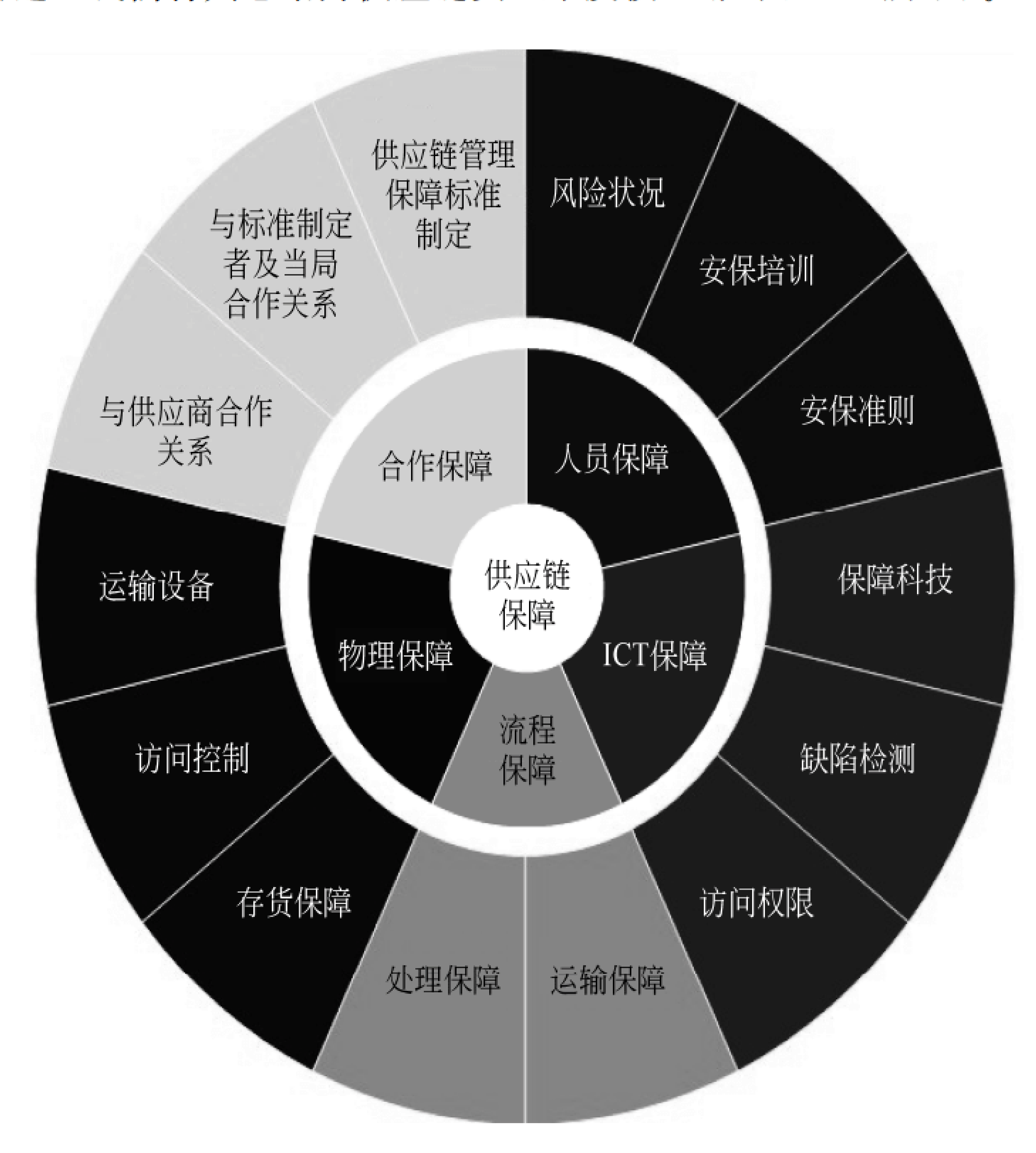


图4-12　供应链安全维度模型的五个维度[TLSSC2011]

表4-4、表4-5、表4-6、表4-7和表4-8通过描述关键的性能指标（KPI）和付诸实践的时间跨度，为每个维度提供一些可行性的建议。这种列表是没有穷尽的，并不是每一个活动都适合所有组织，特别是现行法例，在世界各地各有不同。然而，它作为一个务实的出



发点创造性地思考了如何优化安全态势，可以帮助促进供应链合作伙伴之间的讨论，促进通过共同努力来提高整个供应链的安全。

表 4-4　人员保障措施[TLSSC2011，P41]

保障维度	活　　动	关键绩效指标（KPI）	时间范围
风险状况	为求职者和雇员建立风险状况	筛选过的求职者和雇员比例	2015—2020
	风险状况穷追：定期面谈雇员，每年由警务人员进行许可认证	筛选过的雇员比例	2020—2025
	定期对雇员进行药物检测（一经要求）	吸毒、酒精含量等	2020—2025
	不断地在明处与暗处监督雇员	受观察的雇员比例	2025—2030
安保培训	每年对雇员进行供应链保障培训	参加培训的雇员比例；培训天数	2011—2015
	安保准备程度突击演习	突击演习的数量；参加的雇员比例；突击演习失败的数量	2020—2025
安保准则	雇员安保代号手册	存在性；熟悉度	2011—2015
	举报管理政策，热线	与安保相关的举报数量	2015—2020

表 4-5　ICT 保障措施[TLSSC2011，P41]

保障维度	活　　动	关键绩效指标（KPI）	时间范围
保障科技	对运输资产的感应和传动解决方案	由感应和传动解决方案覆盖的供应链活动比例	2015—2020
	GPS，ZigBee 与运输资产的连接性	GPS 覆盖的供应链活动比例	2020—2025
	无处不在的 RFID 标签（主动和被动）	PFID 覆盖的供应链活动比例	2020—2025
	供应商风险，资源和安全检查的分析型采购工具	采购工具检查和监视的供应商数量	2015—2020
	智能，实时的供应链管理安全事件管理应用	用于核心端到端供应链决策的智能应用数量	2025—2030
	供应链安全机器人	在设施中机器人的数量和功能深度	2025—2030
缺陷检测	以计算机为基础，对供应链保障的破坏和漏洞的模拟	相关测试的结果	2015—2020
	为风险分析和全球货运支持的人工智能应用	相关测试的结果	2015—2020
	无处不在的对 ICT 系统的攻击测试	成功攻击的数量	2011—2015
访问权限	在顾客和执法部门之间分享高风险货运的全球信息	由外部审查者实施的测试的性能结果	2015—2020
	对信息进行加密，防火墙保护和编码	具有先进技术，脚本的基准	2011—2015

表 4-6　流程保障措施[TLSSC2011,P41]

保障维度	活　　动	关键绩效指标(KPI)	时间范围
运输保障	根据 GPS 信号实时地让在危险海域的船只改道	海盗攻击避免的数量	2020—2025
	在运输资产中武装的船员和特殊的武器库站	在船上,飞机上或者铁路资产上武装的船员数量和武器库成员	2015—2020
	合适的时候,托运货物的保险	受保的货物比例	2011—2015
	在产品建造过程中对员工行为的记录	可以追踪到各自雇员的价值附加过程比例	2015—2020
处理保障	自动的分派操作确认检查	在分派操作中自动化检查的比例	2011—2015
	自动的接受操作确认检查	在接受操作中自动化检查的比例	2011—2015
	在各个供应链步骤之间扫描货物	被扫描的货物比例	2015—2020

表 4-7　物理保障措施[TLSSC2011,P42]

保障维度	活　　动	关键绩效指标(KPI)	时间范围
存货保障	存货清单确认	被检查的供应补给比例	2011—2015
	安全库存水平	为供应商和客户作为缓存的库存比例	2011—2015
	存货数量抽查	每年进行的偏差分析数量	2011—2015
	已投保的存货	被保险覆盖的存货比例	2011—2015
访问控制	为人员,生物监测和个性化的访问控制	生物监测和个性化访问控制支持的供应链行为比例	2015—2020
	在物流设施中特别设计的地点	在物流设施中完全被保护的空间大小	2011—2015
	带有 3D 面部识别的智能摄像系统,防偷防盗	在基地部署的智能监控摄像的数量	2025—2030
	对严格限制地域或者货物的控制访问	可以访问限制地域或者货物的人员比例	2015—2020
运输设备	对装载的单元封装	装载单元被封装的比例	2011—2015
	电子封装/智能集装箱/智能运输资产	配备有电子封装的集装箱比例	2015—2020
	特殊设计的运输保障资产开发	在船队中特殊设计的传输保障资产比例	2020—2025

表 4-8 合作保障措施[TLSSC2011,P42]

保障维度	活　　动	关键绩效指标(KPI)	时间范围
与供应商合作关系	供应商强制保障认证	被认证的供应商比例	2015—2020
	替代供应商的能力	从一个供应商转换到另一个供应商的时间	2011—2015
	分层供应网络的完整可见性(供应商的供应商)	透露其供应商的供应商比例;来自高风险地区的供应商比例	2015—2020
	供应商价值附加过程的跟踪和检查	在供应商过程中货物跟踪的比例	2015—2020
	战争赌博实践	在战争赌博练习中的表现	2015—2020
与标准制定者和当局合作关系	100%服从 AEO/C-TPAT 要求	100%服从 AEO/C-TPAT 的供应链伙伴数量	2011—2015
	强制 ISO 28000	ISO 28000 指定的供应链伙伴数量	2015—2020
	对所有货物船运的集中数据储存和100%的所有全球船运信息储存在中心数据库中	通过中心数据库的货运数据流	2015—2020
供应链管理保障标准制定和实施	风险识别和分析	覆盖/受保的风险比例	2011—2015
	应急措施	有准备的应急计划数量	2011—2015
	后危机管理	反应中断所要求的时间	2015—2020

运输和物流行业已经十分依赖信息和通信技术(ICT)的趋势正不断上升。虚拟威胁应该与物理威胁受到了同等重视。引发物理破坏的网络攻击将越发成为运输和物流行业的威胁。网络攻击的破坏不仅仅只是虚拟性的。网络攻击可以导致物理破坏。这是因为信息系统同时也控制着重要的功能,比如航空交通控制。因此命令也可导致人为的机能故障,进而引起巨大的破坏。所以保证网络空间安全以成为刻不容缓的事情,应该引起足够的重视。

4.5 NIST 系统开发生命周期模型

为了促进《联邦信息管理法案》(FISMA)的实施,满足保护联邦信息系统的安全需求,NIST 发表了一系列的特殊出版物(NIST SP),它认识到在系统开发生命周期中的安全考虑对于管理组织中信息技术资产全面策略的实施和集成是至关重要的。NIST SP 800-64 就是为了协助联邦政府机构将必要的安全活动整合到他们建立的系统开发生命周期中而发布的。这个指南的目的是协助相关机构在 IT 开发进程中嵌入安全措施,它主要关注系统开发生命周期(Systems Development Life Cycle,SDLC)的信息安全组件,至于整个系统的实现和开发以及机构的信息系统管理进程都不做详细论述。NIST 系统开发生命周期模型是由美国国家标准与技术研究所(NIST)在其出版物 NIST SP 800-64 中提出的。模型首先描述了大多数信息系统开发中关键安全角色和职责,然后将安全措

施纳入系统开发生命周期(SDLC)的各个阶段。

4.5.1 系统开发生命周期

SDLC 的全称为系统开发生命周期(System Development Life Cycle),包括如下5个阶段(如图4-13所示)。



图4-13 SDLC的5个阶段[NIST2008]

(1) 启动(Initiation):SDLC 的启动阶段,最基本的活动是定义信息系统需求。该系统的发起者已经确认,该系统连接到一个或多个组织目标,能够被信息系统解决的问题的初始定义已被文档记录。在这个阶段的步骤包括建立基本的系统思路,初步需求定义,可行性评估,技术评估和确定管理人员以进入下一个阶段。

(2) 采购/开发(Acquisition/Development):在获取/开发阶段,系统需求被收集并验证。一些系统组件可能是从商家采购,一些是内部建立的。大部分的安全规划发生在这个阶段。

(3) 实现/评估(Implementation/Assessment):在实现阶段,新的信息系统被测试并投入初始生产模式。

(4) 操作/维护(Operation/Maintenance):在操作/维护阶段,信息系统正常生产运行,系统变化和更新被掌控。

(5) 处理(Disposal):在处理阶段,信息系统从生产中移除并退休。

SDLC 贯穿多重连续过程开发信息系统的全过程,该过程包括需求分析、设计、开发、测试、维护和最终的退休。应用 SDLC 模型可以增加项目成功的可能性,尤其是在满足管理领域需求方面。在开发早期识别安全需求并把它们纳入到整个系统开发生命周期SDLC 中,开发系统的安全目标将很容易实现。

当不可能从组织运营中估算出所有的风险,保护组织资产的最有效的方式之一是将安全纳入系统开发生命周期(SDLC)。在 SDLC 中嵌入安全措施,组织可以获得三个关键的益处:第一,也是最重要的,系统可以从强大的安全性中获益,减少开发脆弱的可能

性和/或影响;第二,在 SDLC 的相应阶段考虑对应的安全措施,将安全嵌入到系统中将使系统的安全性实现无缝对接而且可以减少花费,相反,用安全需求改装系统可能是一项高额的进程;第三,将安全嵌入到联合信息系统的生命周期中是认证和认可进程(C&A)的要求。

4.5.2 模型的基本原理

已有的 SDLC 模型包括瀑布模型、喷泉模型、螺旋模型、边做边改模型、快速原型模型、增值模型、同步安定模型。这里选择瀑布模型,原因在于,它是应用最广且最被广泛接受的模型。几乎所有其他模型都源自于瀑布模型,它的线性流程可以很容易展示将安全嵌入哪个阶段,没有使用瀑布模型的组织能够很容易将这里提到的规则转换到他们所选的 SDLC 模型中。

下面将在 SDLC 中嵌入详尽的安全措施形成 NIST 系统开发生命周期模型。

1. 启动

启动阶段包括用于确认所有利益相关者的不同需求的活动,如图 4-14 所示。包括定义利益相关者,利益相关者面谈,使用案例或者一些基本的原型设计。在本阶段的结尾,所有对设计和购买系统必要的需求都应该被识别和完全理解。本阶段对安全需求的识别非常重要,下面的安全措施(表 4-9)有助于确保安全需求被恰当识别。

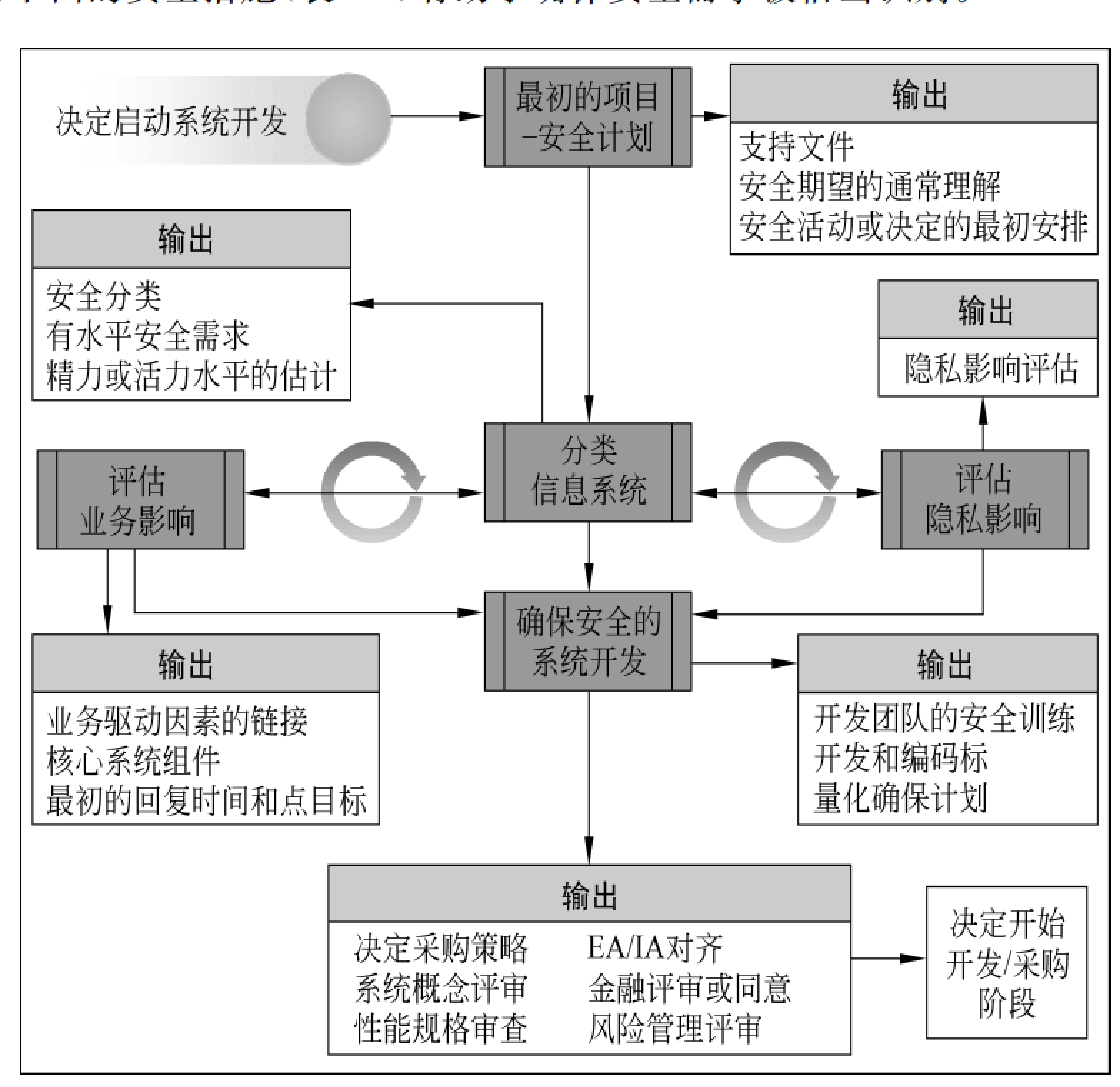


图 4-14 将安全考虑纳入到启动阶段[NIST2008 P19]

2. 开发和获取

在开发和获取阶段,功能和技术需求转化为对实际信息系统的详细计划,如图 4-15 所示。使用案例和实体模型发展成为顺序图、行为图、状态图和其他可以被软件程序员解读的人工产品,对用户接口进行了更加详细的描述,安全需求应该被纳入到系统设计。相关措施如表 4-10 所示。

表 4-9　在启动阶段的安全措施[OnPoint P3]

安全措施	描　述
识别安全类型 (参考 NIST SP 800-60)	列举系统的信息类型可以强档构建安全需求。联邦信息系统,NIST SP 800-60 是识别不同信息类型的参考,由于它与美国联邦组织架构(FEA)企业参考模型相关。NIST SP 800-60 中列举的每一种信息类型都有一个建议的安全影响水平和理由
执行隐私阈值分析 (参考 OMB M 03-22)	个人验证信息的保护是联邦政府的一大担忧。在需求分析阶段通过执行隐私阈值分析,联邦机构将能单独为个人验证信息需求做计划。这个分析也有助于确定需要构建什么类型的隐私影响评估(PIA)以及该系统是否符合 1974 隐私法
信息系统分类 (参考 NIST FIPS 199)	在系统的信息类型被确认以后,安全分类和相应的系统影响水平就可以被确定。安全分类测量当三个安全目标(机密性,完整性,可用性)的任何一个遭受攻击使组织受到的潜在影响。每个安全目标的影响被测量为低等,中等,高等。FIPS 199 为这个过程提供了指导。为了获取全部整个影响水平用于指挥安全控制部分,在这三个目标之间会标记高水位
选择安全控制 (参考 NIST SP 800-53)	在所有信息类型被确定,并且安全分类完成必须进行安全控制的选择。NIST SP 800-53 将控制分为三个基准线来对应潜在的系统影响水平(低,中,高)。系统拥有者可以使用 NIST SP 800-53 来确定需要应用于信息系统的安全控制的裁剪。然而,仍然需要另外一层裁剪。组织将要进行确认的控制中,有一些是不可以应用的,还有一些是没必要的。那些被认为是没必要的,应该确定补偿性控制,残余风险必须被接受。而且,由于 SP 800-53 阐述了管理的、操作的、技术的概念,许多控制不能应用于系统的开发,但是可以应用于系统的管理和操作

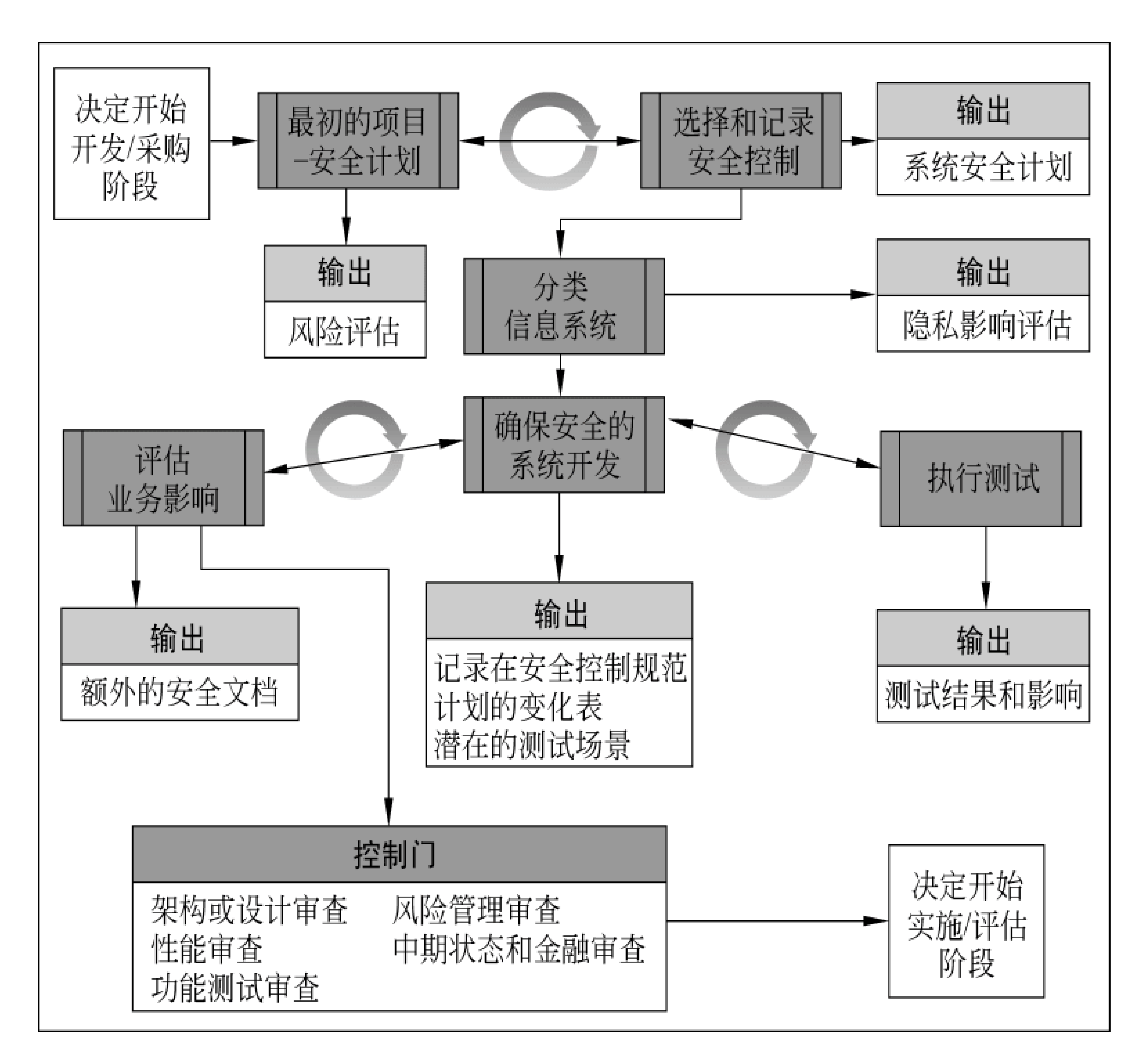


图 4-15　将安全考虑纳入到开发和获取阶段[NIST2008 P27]

表 4-10　在开发和获取阶段的安全措施[OnPoint P4]

安全措施	描　　述
开发安全架构（参考 NIST SP 800-53）	开发安全架构包括决定每个安全需求是如何被满足的。例如，许多安全需来自于外部实体。例如，防火墙、入侵检测系统(IDS)和活动目录安装可能是由外部服务组织提供的。其他的，例如审计功能和输入验证，需要在应用中开发。安全架构将在需要安全控制的地方出现并确定需要安全控制的组织
执行初始风险评估（参考 NIST SP 800-30）	在这个阶段执行风险评估将有助于组织再次评估计划的安全态势是否符合系统和系统中存放的信息的需求。通过确定威胁、脆弱点和它们潜在的影响，组织可以确定在实施完安全控制后残留风险是否可接受。这是昂贵的开发前有效的立见分晓的检验
开发系统安全计划（参考 NIST SP 800-18）	系统开发到此时已经足以开始创建系统安全计划(SSP)。系统安全计划是系统 C&A 的关键部分。由于所有的联邦系统需要经过 C&A 优先开发，创建系统安全计划将使系统开发加速进入成品环境。此外，SSP 需要的大部分信息在分析和设计产品过程中将被详细说明
评估商业影响和执行应急计划（参考 NIST SP 800-34）	在开发和获取阶段就应该知道要为系统计划机密性。通过构建商业影响评估(BIA)和开展机密性计划，系统一经部署组织将能够对破坏做出恰当反应

3. 实施和评估

实施由信息系统的实际编码组成，如图 4-16 所示。前两个阶段创建的所有分析和设计成果都由程序员转换成实际编码。本阶段仍然会有初步测试和调试。实施和评估阶段的产物是工作应用。利用在开发和获取阶段完成的安全架构，程序员应该准确地知道他们在实施技术安全控制中的职责所在。这个阶段的评估部分包括通过用户验收核查用户

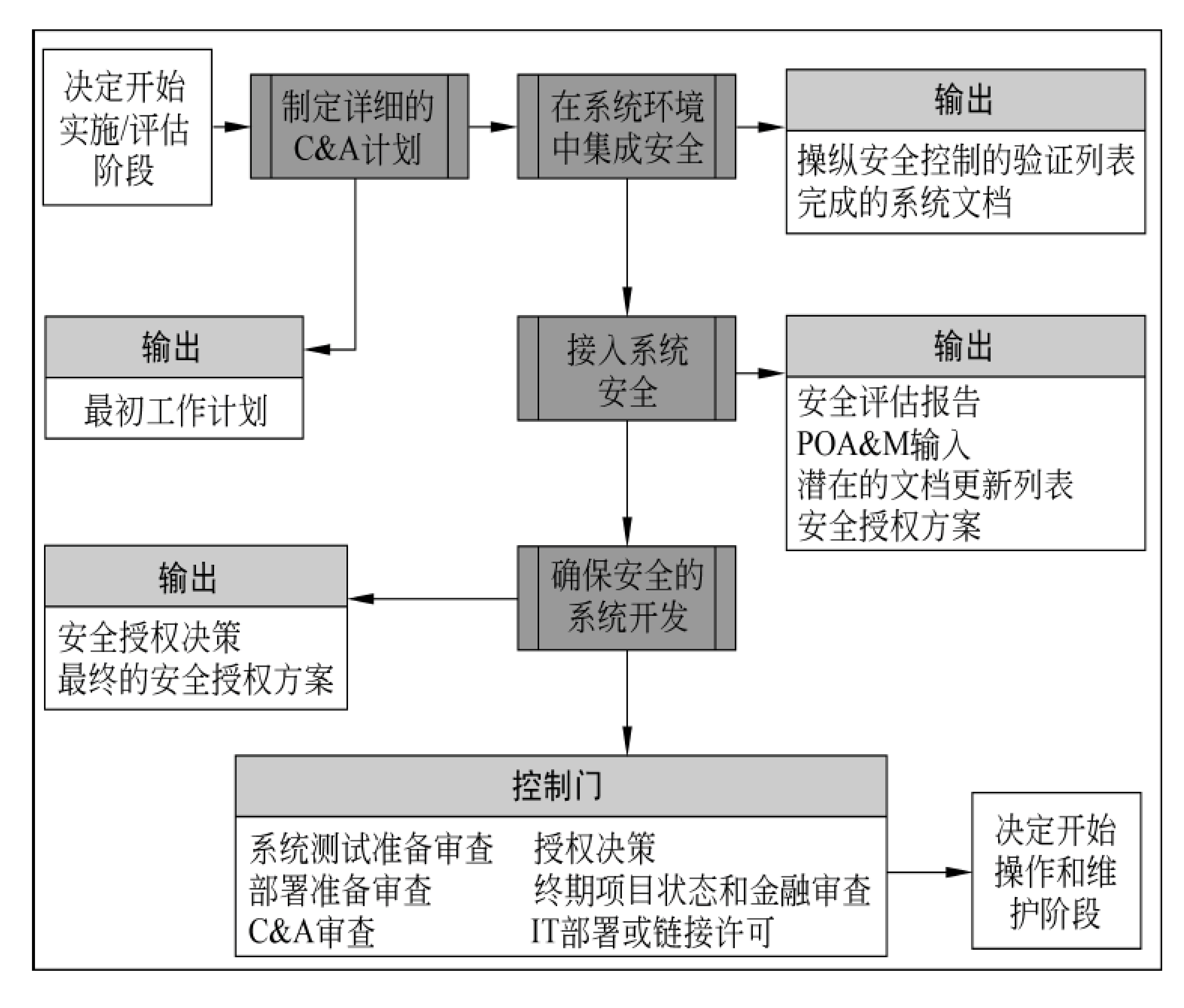


图 4-16　将安全考虑纳入到实施和评估阶段[NIST2008 P34]

功能,质量确保测试,登录测试以及其他一切确保工作按计划执行的技术测试。一旦验证完成,这个系统就会进入成品环境。相关措施如表4-11所示。

表4-11 在实施与评估阶段的安全措施[OnPoint P5]

安全措施	描述
联合技术最佳实践 (参考 DISA STIGS)	可应用的最佳实践应该用于已选择的开发技术,不论它是网络动态伺服页,Java,应用服务器平台等。优秀的程序员能够理解最佳案例,并默认包含它们
结束系统安全计划 (参考 NIST SP 800-18)	如果系统在SDLC之前的阶段里被恰当记载,那么结束SSP将是一项小任务。如果需要大体改变,或许意味着设计方案不能实施。有时是由于技术限制。由于系统的设计已经完成,SSP应该反映它的产品状态
开发安全控制测试计划 (参考 NIST SP 800-53A)	测试安全控制是C&A和成为最佳案例的要求。设计的测试计划应该反映SSP中提供的信息。测试计划不应该包括对外部系统提供的控制,不可用控制,被认为没必要的控制以及已经被认为无效或者不恰当的控制的测试
测试安全控制 (参考 NIST SP 800-53A)	在释放系统之前必须确定SSP中记录的所有安全控制是恰当的和有效的。这项工作通过执行安全控制评估来完成。按照之前实施阶段开发的测试计划执行。测试结果,尤其是那些没有通过的控制应该被记录
开发 POA&M (参考 NIST SP 800-37)	行动计划和里程碑是另一个重要的C&A文件,它详细记录了通过文件分析和测试确认的所有缺陷。它提供了弥补缺陷和需要资源的时间表
授权系统 (参考 NIST SP 800-37)	这是在系统开发前的最后一个步骤。一旦完成,系统将要进入瀑布SDLC的操作/维护阶段。系统所有者将向组织授权官员出示授权包。这个授权包将包含所有的C&A相关的人工产品,包括SSP、安全评估文档以及POA&M。根据已有信息,授权官员将决定系统的命运。如果剩余风险是可以接受的,系统将获得授权投入生产。为了加快系统开发,要在瀑布模型的每个阶段实施完成相应的安全措施。经常出现这种情况,安全措施率先进入SDLC。这将导致文件之后和无效的安全控制

4. 操作和维护

操作和维护包含使系统按要求工作所需要的所有活动,如图4-17所示。它包括硬件的定期维护、补丁管理以及应用错误补救,不包括用户功能升级。额外的功能需要进入需求分析阶段。操作/维护阶段在产品环境下与系统一直共存。相关措施如表4-12。

表4-12 在操作/维护阶段的安全措施[OnPoint P6]

安全措施	描述
管理配置变化 (参考 NIST SP 800-53a)	在系统进入生产环境之前,要对配置进行快照并评估安全性。如果配置变化了,那么有效的安全性也会变化。在操作/维护阶段,组织必须跟踪所有配置修改并评估有效安全性的变化
修复 POA&M 项目 (参考 NIST SP 800-37)	通常,系统在接受了授权操作后仍然存在安全缺陷。创建POA&M来提供修复缺陷的计划。在操作/维护阶段,安全缺陷按照日程表和POA&M中列出的优先次序被修补

续表

安全措施	描述
安全控制再测验 **(参考 NIST SP 800-37,SP 800-53a)**	为了确保在安全授权过程中的评估部分测试的安全控制仍然是恰当的,按照计划运行,得到需要的结果,组织每年需要重新测试一部分控制。目标是使所有控制每三年再测试一遍。这在 NIST SP 800-37 rev.1 中得到了很好的展示。在授权结束阶段,组织可以使用在维护阶段进行的再测试来完成安全授权过程中的安全控制评估需求
执行操作安全 **(NIST SP 800-86,NIST SP 800-83,NIST SP 800-61,NIST SP 800-40)**	操作安全是由信息安全群组执行的日常安全措施组成的集合。一些显著的安全措施包括: • 管理和监视防火墙/IDS/安全设备 • 事故应答 • 补丁管理 • 脆弱性管理

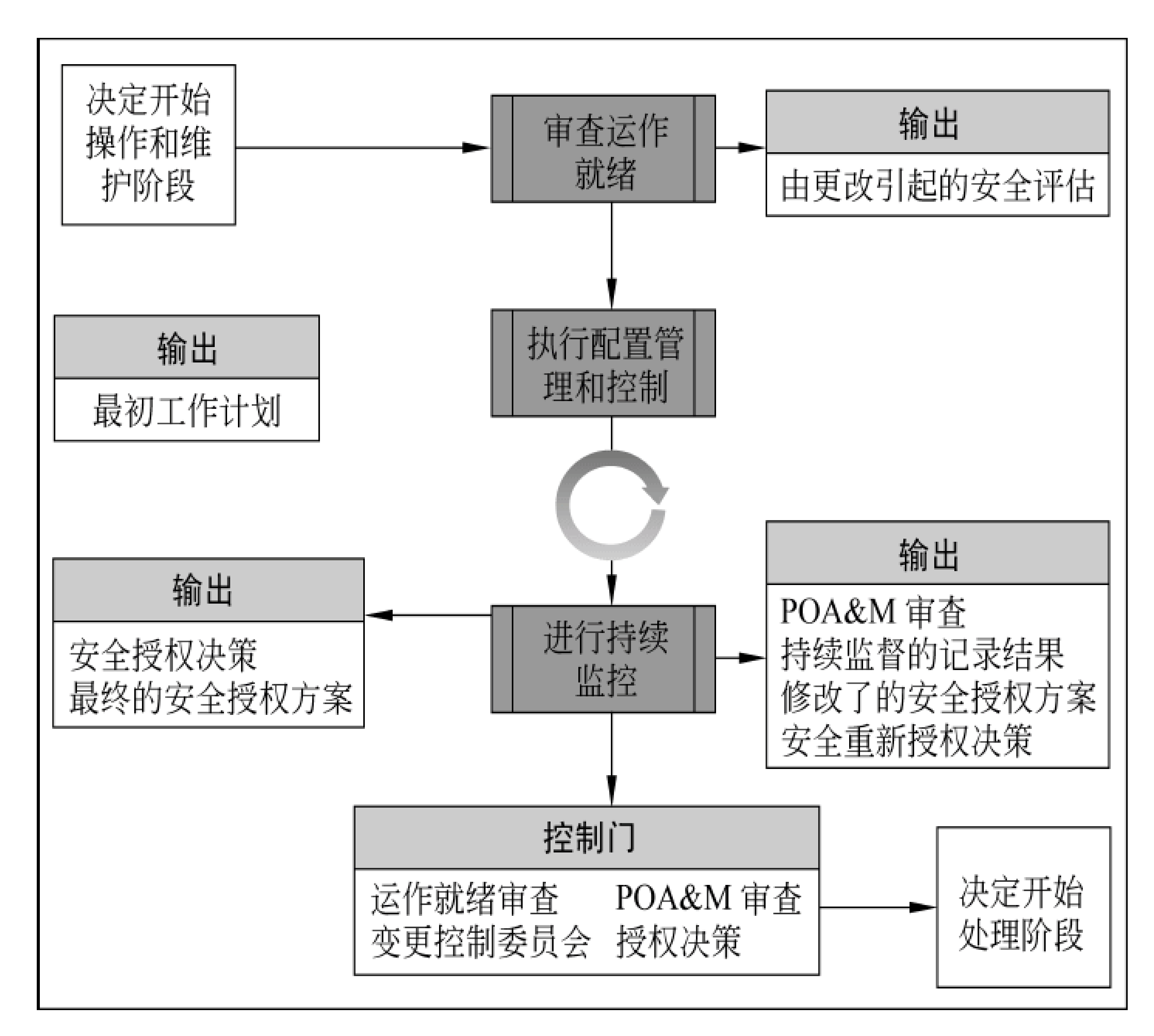


图 4-17 将安全考虑纳入到操作和维护阶段[NIST2008 P38]

5. 处理

处理出现在系统需要被替换或者功能不再被需要的时候,如图 4-18 所示。在处理阶段,系统脱离生产,使它不再接触用户群体。相关措施如表 4-13。

表 4-13 在处理阶段的安全措施[OnPoint P6]

安全措施	描述
保存信息 **(NIST SP 800-111)**	不定期地,系统退休后,系统中的数据必须维护一段时间。这是管理机构的要求或者信息所有者的要求。保存信息程序很重要,同时要进行相应敏感水平的保护

续表

安 全 措 施	描　　述
清理媒体 （参考 NIST SP 800-88）	为了再利用或者摧毁媒体，作为安全措施媒体清理经常被忽视。通过专业服务和 COTS 产品进行数据恢复的升级使媒体被清理还是通过认可的方法摧毁很重要。没有正确处理的媒体可能象信息漏洞威胁暴露代理

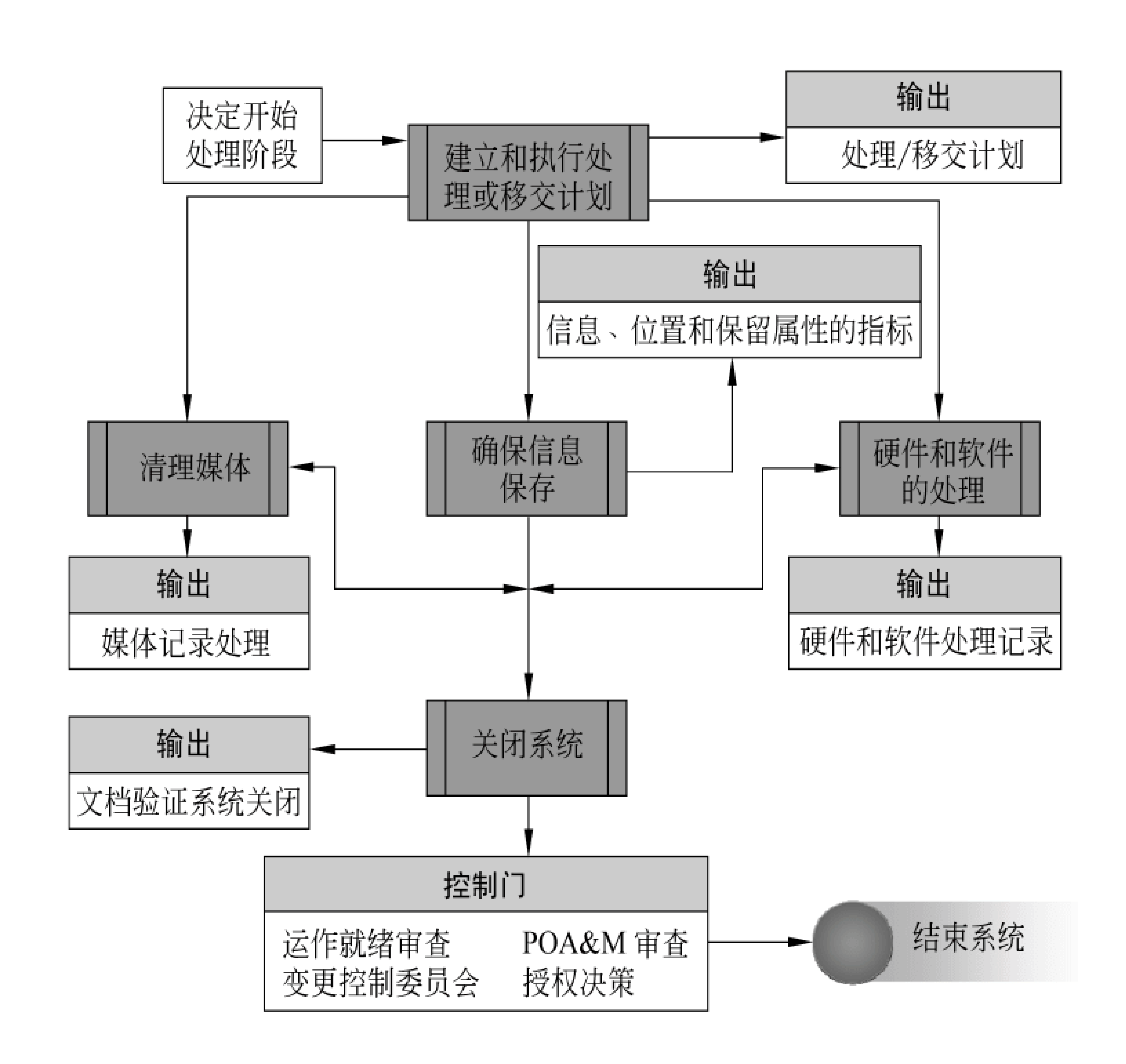


图 4-18　将安全考虑纳入到处理阶段[NIST2008 P42]

SDLC 有助于确保信息系统的成功开发、操作和退休。SDLC 在许多组织中缺少的是信息安全措施的明确嵌入。OnPoint 建议负责代理信息安全工作的个体应该与系统设计者和开发者密切合作以确保恰当的安全需求被纳入到 SDLC 的所有阶段中。通过成功地将安全纳入 SDLC 的不同阶段，组织机构在纳入安全方面可以节省资金，提高系统安全性，从整体上降低代理可接受的残余风险。

4.5.3　模型的应用

本节通过案例的方式帮助读者理解安全在系统开发生命周期中纳入安全措施的重要作用，展示如何将安全纳入到 SDLC 的每个阶段。如果安全被纳入到 SDLC 的每一个阶段，那么信息系统将是默认安全的，之后系统的变化不太可能引起总体的安全隐患。

案例研究的对象是 GIAC Bikes 客户信息系统。GIAC Bikes 这家公司设计并以零售和网售的方式出售爬山车。在自行车市场，Bad Bikes 是 GIAC Bikes 的主要竞争对手（过去 Bad Bikes 曾试图剽窃自行车设计方案和攻击 GIAC Bikes 网站）[BSSDLC]。

1. 启动阶段[BSSDLC]

案例研究：在 SDLC 启动阶段，GIAC Bikes 定义了顾客信息系统需求。系统的

GIAC Bikes 需求可以使它更好地追踪顾客的购买习惯和喜好从而更好的规划未来自行车设计和市场计划。

GIAC Bikes 系统开发团队在本阶段采取的安全措施是基于对信息系统的初步风险评估而进行的安全分类。安全分类显示了顾客信息系统的机密性、完整性和可用性(confidentiality，integrity and availability)对 GIAC Bikes 的重要性。

设计团队关注危险地带，包括所收集的信息的敏感性，对 GIAC Bikes 的系统临界，对客户信息系统普遍的安全风险以及与客户信息系统相关的规则、法律和隐私问题。该系统设计团队对每个风险区域分配高媒介低风险值。例如，因为 GIAC Bikes 经营在欧洲(一个隐私法律很强大的地方)，客户信息系统搜集了个人数据，风险和系统信息高机密性的影响。另一个例子是尽管客户信息系统对 GIAC Bikes 非常重要，如果系统很长时间不可利用经营仍然可以持续。所以设计团队对系统可用性赋予低风险值。GIAC Bikes 已经知道 Bad Bikes 曾经攻击过它的电脑系统，所以也预料到将来会有新的攻击。

将初步的风险评估作为建立系统需求的一部分有助于在以后的 SDLC 阶段投入大量时间和精力之前识别出所有安全隐患，这可以使设计团队在设计过程早期思考安全问题。

2. 获取/开发阶段[BSSDLC]

案例研究：在 SDLC 获取/开发阶段，GIAC Bikes 开始设计完整的顾客信息系统(在此案例中 GIAC Bikes 决定购买一个客户信息系统)。详细的需求被收集并验证。获取和开发均被考虑并做出最好的选择。基于对系统需求的分析和可用选择，GIAC Bikes 启动了征询方案(Request for Proposal，RFP)程序以从第三方供应商获取一个顾客信息系统。

随着越来越多的详细系统需求被搜集和验证，GIAC Bikes 在最初的风险评估的基础上加以扩展以便包括新的详细需求。GIAC Bikes 将安全需求纳入到 RFP 的服务水平协议(Service Level Agreement，SLA)中。例如，GIAC Bikes 决定通过在用户应用程序中使用基于角色的访问控制系统来实现客户信息系统的关税分离，这样，需求在 RFP 中被记录。GIAC Bikes 还指定了内部安全控制来降低风险。系统管理员将进行新的背景调查。敏感客户信息的收集系统备份将被加密。一个入侵防御系统(intrusion prevention system，IPS)将被添加到 GIAC Bikes 网络中来防止对顾客信息系统的网络攻击。GIAC Bikes 还在这个阶段开发了一个测试计划以确保所有的计划安全控制功能如指定的那样实施。

由于新的客户信息系统需要集成到其他 GIAC Bikes 信息系统(如会计系统)，GIAC Bikes 将检查所有的集成点并寻找引入的新的安全风险。新的和改进的控制被计划用以应对集成问题。例如，决定使用 IPSEC(网际协议安全，Internet Protocol Security)身份验证和加密由顾客信息系统服务器传输到会计服务器的任何数据。

3. 实现阶段[BSSDLC]

案例研究：在实现阶段，GIAC Bikes 安装了新的客户信息系统并开始测试所有的系统功能。这个测试包括检查在获取/开发阶段所有指定的安全控制能否如设计的那样运行。对所有 GIAC Bikes 其他系统的集成点都进行测试。客户信息系统的用户在新系统上接受训练。这个训练包括最新的安全意识训练。在 GIAC Bikes 案例中，员工接受关

于如何保护客户私人信息的训练。他们还接受如何识别和抵制社交工程攻击的训练。GIAC Bikes 风险评估显示为了获取客户个人信息的社交工程是一个主要风险。GIAC Bikes 顾客信息系统正在经历一个调整,所有的系统功能(包括安全)通过测试和验证被确认,GIAC Bikes 高级管理正式接受(授权)系统投入生产。

4. 操作/维护阶段[BSSDLC]

案例研究:在操作/维护阶段,GIAC Bikes 开始对客户信息系统的定期生产运作。由于 GIAC Bikes 从外部供应商购买了客户信息系统,本阶段的大部分任务是检测系统的性能以确保系统满足购买时指定的服务水平协议(SLA)。系统的更新和加强必须被评估并在需要时加以应用。

本阶段采取了特定的安全行动以确保对系统的任何更改都需要通过 GIAC Bikes 配置管理过程。GIAC Bikes 监视和审计客户信息系统以寻找任何未经授权的系统更改。任何建议的系统更改需要进行安全影响评估。例如,供应商发布一个 Oracle 数据库的新版本的系统升级,GIAC Bikes 确定新版本需要一个新的数据库服务器,它将必须确保这个新的数据库服务器完全满足客户信息系统安全需求。GIAC Bikes 监视的另一种类型的系统更改是用户角色,它使用基于角色的访问控制来满足系统中的关税分离的安全需求。综上 GIAC Bikes 通过监视用户访问更改以确保"访问蠕变"没有发生以及用户不能获取工作需要以外的更多访问权(最小特权)。

5. 处理阶段[BSSDLC]

案例研究:部分 GIAC Bikes 的客户信息系统一直在升级或者更换。GIAC Bikes 进行配置阶段安全活动。例如,当原来的数据库服务器为了 Oracle 数据库升级换成了新的模型,GIAC Bikes 验证旧数据库系统成功地转换成新系统以及客户信息系统或者交易事物没有丢失或误传。在原来的数据库服务器再利用或者处理之前,GIAC Bikes 使用磁盘驱动器来删除所有的客户信息系统数据的踪迹。

6. 总结[BSSDLC]

这个案例研究贯穿了 GIAC Bikes 客户信息系统的整个系统开发生命周期,列举了 SDLC 的每个阶段的安全措施,有助于帮助读者更加深刻地理解忽略了 SDLC 系统的任何阶段的安全措施都会严重危害系统的安全。

4.6 达沃斯-供应链和运输风险模型

2011 年达沃斯年会之后,世界经济论坛邀请了不同领域的专家就供应链和运输系统的脆弱性展开探讨。此篇关于供应链和运输风险的报告对已经讨论过的外部冲击、发展趋势及系统脆弱性等内容进行了回顾。报告提出了多种风险缓解方法,以便进一步拟定行动建议。2012 年达沃斯年会以"新形势下的共同准则"为主题,围绕应对新形式、经济前景和制定包容性增长政策、支持二十国集团的行动计划以及建立全球风险应对机制四大议题展开了讨论。论坛聘请了各种供应链和运输风险专家来探讨系统性缺陷,发布了供应链和运输风险报告,回顾了外部冲击,网络趋势和漏洞。本节将介绍达沃斯年会对供应链安全的讨论以及供应链和运输风险模型[WEF2012]。

4.6.1 模型的产生背景

随着国际形势的发展和变化，世界经济论坛所探讨的议题逐渐突破了纯经济领域，许多双边和地区性问题以及世界上发生的重大政治、军事、安全和社会事件等也成为论坛讨论的内容。为填补全球网络风险防范空白，2011 年的达沃斯经济论坛正式推出全球风险应对机制，以应对各种相互关联的复杂风险。据了解，目前还没有一个全球网络或全球机制能系统总结防范风险的策略与经验，并为所有管理者及时、合理制定决策提供依据。而在全球化中，人类面临的风险呈现多样化、关联化和复杂化趋势，风险发生后如不能及时、合理应对，易造成全球性影响。为解决上述问题，本届达沃斯论坛正式推出全球风险应对机制，以增强人类应对自然风险和人为风险的能力[WEF2012]。

全球供应链和运输网络形成了全球经济的骨干，推动贸易、消费和经济增长。全球化、精益流程和生产的地理集中的趋势使供应链网络更高效，但也改变了他们的风险状况。大多数企业拥有可以预防局部中断的风险管理协议。然而，最近高调的事件凸显出各个组织的控制之外的风险可以引起级联和意想不到的后果，这种后果一个单独的组织无法缓和。供应链和交通中断已不再被仅仅视为操作风险管理者的权限。在 2008 年全球金融危机和其他主要供应链中断的浪潮中，智力模型的改变推动了组织审查自己的方法以识别和减轻系统性风险。高级别的领导和公司董事会正越来越多地理解和负责组织风险的许多方面。政府在全球供应链和运输网络的风险理解和管理也已经越来越受到挑战。政治、经济和安全在复杂环境中调节的影响成为公共私人合作的新方法[WEF2012]。

4.6.2 模型的基本原理

供应链和运输提供者需要在采购、运输和分销链等多个环节管理风险。在相互联系的世界上，安全、可靠性和效率只能依靠行业及政府之间的合作来实现。从恐怖主义、天气、货币到信息技术的弊端，需要一个实用的框架来汇集不同的风险，帮助政府或者企业定义风险的优先级。针对供应链和运输的现状，2011 年的达沃斯论坛上提出了降低风险的策略以进一步开发和阐明行动建议，形成了供应链和运输风险模型[WEF2012]。

1. 理解供应链和运输风险的暴露

在供应链和运输网络中的系统风险被描述为意想不到的突发事件，网络设置不能吸收冲击和连锁效应。最初事件可能会导致级联中断或者跨地区或行业的失败。然而，对中断的预测没有在任何情况下有效应答的恰当弹性那么重要。专家们定义了限制供应链和运输网络弹性外部的干扰和漏洞（如图 4-19 和图 4-20 所示）。

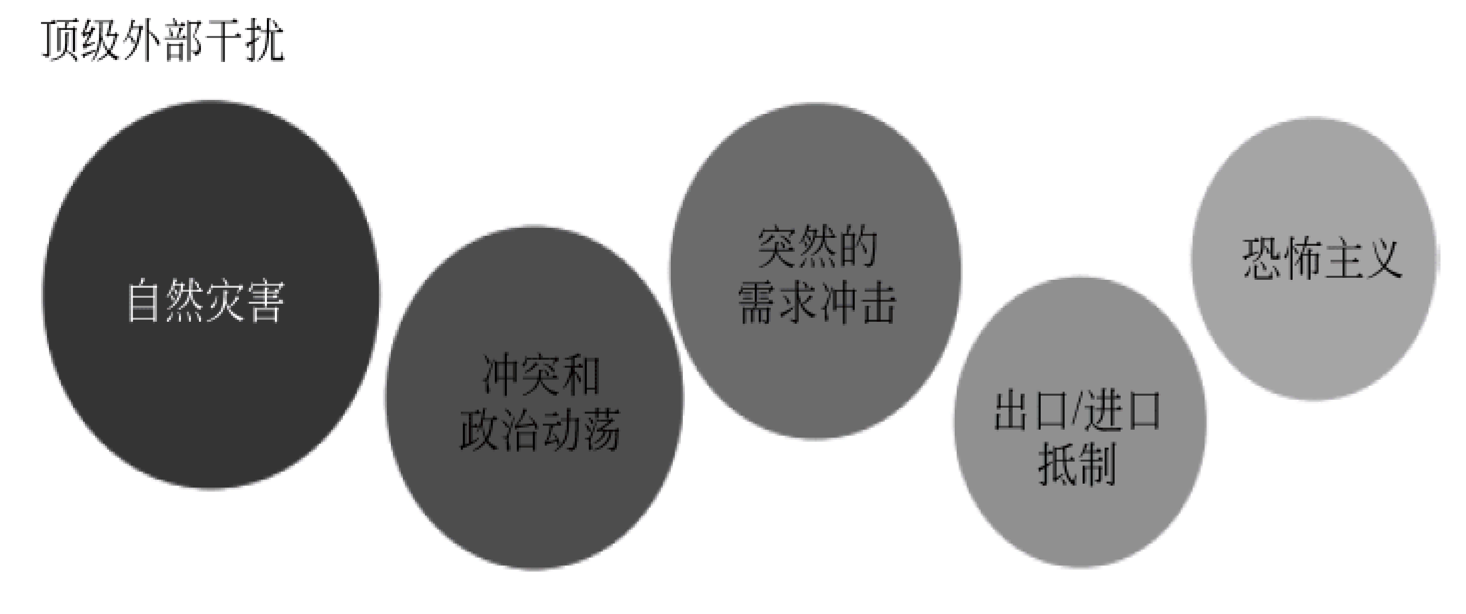


图 4-19 顶级外部干扰[WEF2012 P4]

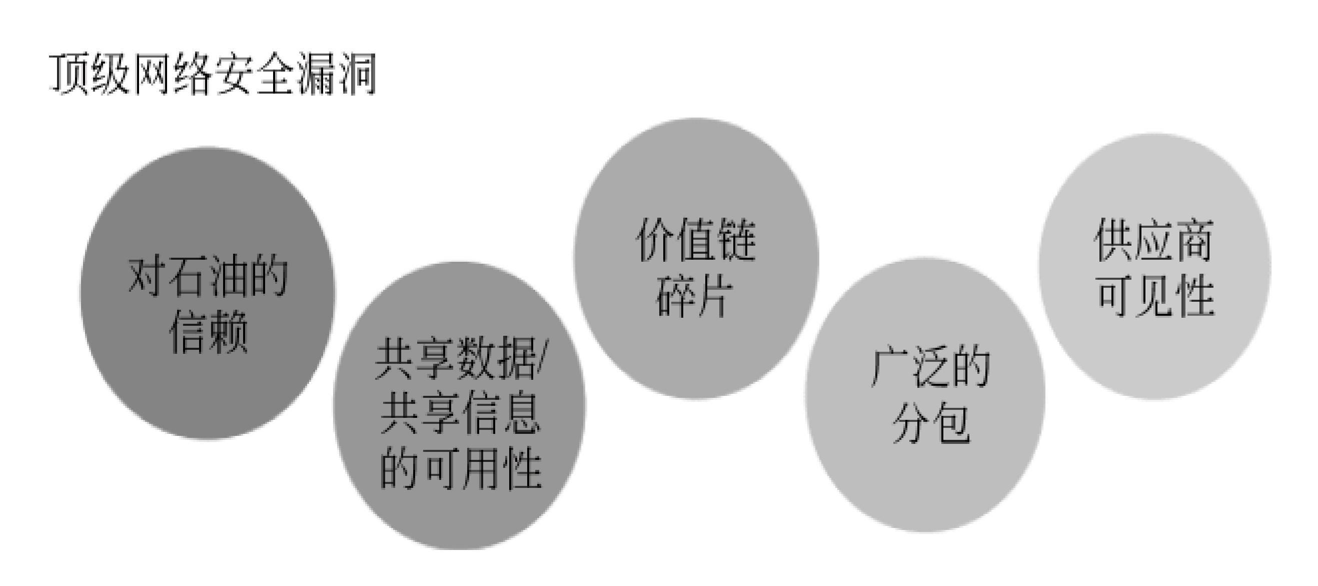


图 4-20 顶级网络安全漏洞[WEF2012 P5]

2. 实施改进的系统性风险管理

专家组评估了当今可用的风险管理方法和将来最重要的方法之间的差别从而确定了发展最需要的风险管理方法(如图 4-21)。

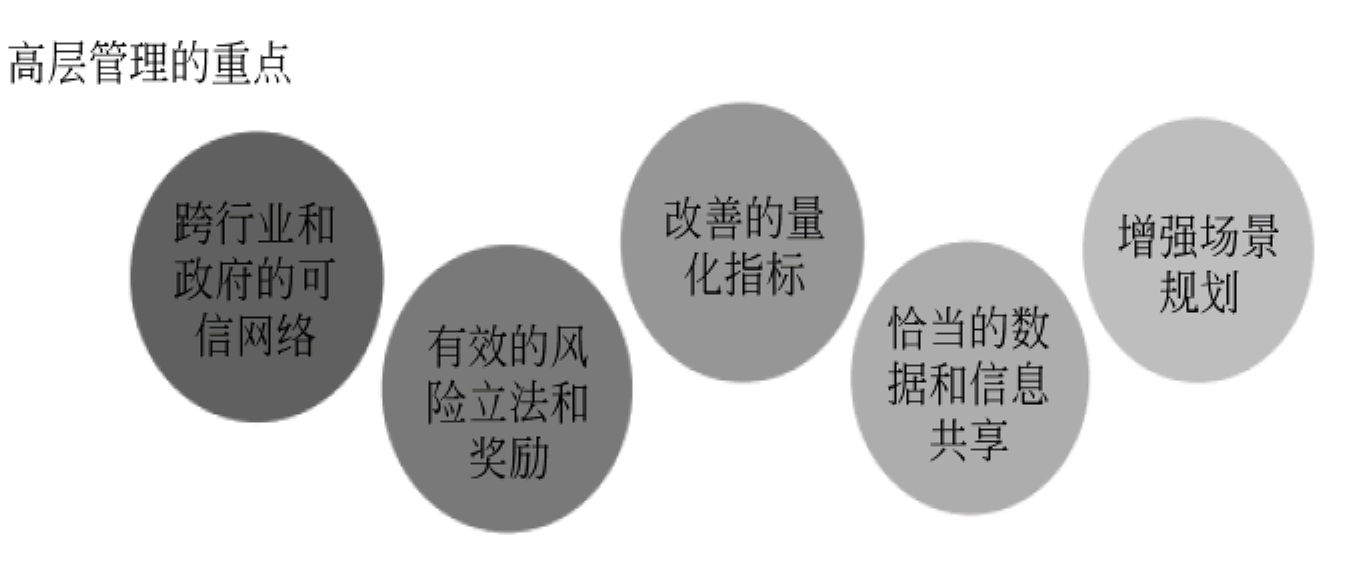


图 4-21 高层管理的重点[WEF2012 P5]

3. 降低风险并建立弹性

为了有效地管理供应链和运输风险,更大程度的合作是必要的。专家鉴定了大量的需要有效管理系统供应链和运输风险的优先领域(如图 4-22),关注如今可用的风险管理方法和未来最重要的风险管理方法之间区别的调查分析。

这些优先风险管理领域并不是相互排斥的:把这些工具作为管理措施集合的组成部分,可以更有利于风险管理的实施。如图 4-23 是企业和政府首先应该确认和开发可以促成有效合作的必不可少的风险措施集合。

不同公共和私人的部门实体的汇合将允许更大程度的数据和信息共享,使组织更好地理解和量化供应链和运输风险。这反过来将暴露公共的和私人部门在漏洞领域的投资并促进积极和有效的立法的发展,对来自跨公司、地区和情景规划部门的关键方的合作也有同样的作用。下面给出具体的风险管理措施。

1) 建立跨业务和政府的可信网络[WEF2012]

跨越端到端的供应链系统风险的有效识别和管理需要企业、专业机构、政府、监管机构、供应商、顾客甚至是竞争对手之间的高水准合作。严格管理的信息、专长和优先权的共享可以发展合作和信任关系,这种关系对于中断前的准备和中断后的迅速反应以及改善其他四种风险管理方法至关重要。企业和政府对在全球范围内扩大供应链和运输风险上的合作有极大热情,这意味着全球中断会带来很多经济、安全和政治问题,所以需要采取一种隐蔽的方法来进行风险管理。然而,焦点地带优先级的调整和达成一致将不可避免的是一个渐进过程而且需要来自公共的和私人部门领导人的大量投入。在工业和/或

风险管理优先级

改进重点

风险量化指标

业务连续性计划

情景规划

数据和信息共享

集中的风险管理程序

跨业务和政府的可信网络

以商业为主导的质量标准

专业认证和授权

供应商审核协作

新的立法

符合环保及安全法规

培训和教育

事件管理工具

追踪和跟踪工具

行业标杆研究

政府刺激计划

财务风险累积的费用

供应生厂商合规考核

保险

未来的重要性

有待提高

图 4-22　需要有效管理系统供应链和运输风险的优先领域［WEF2012 P15］

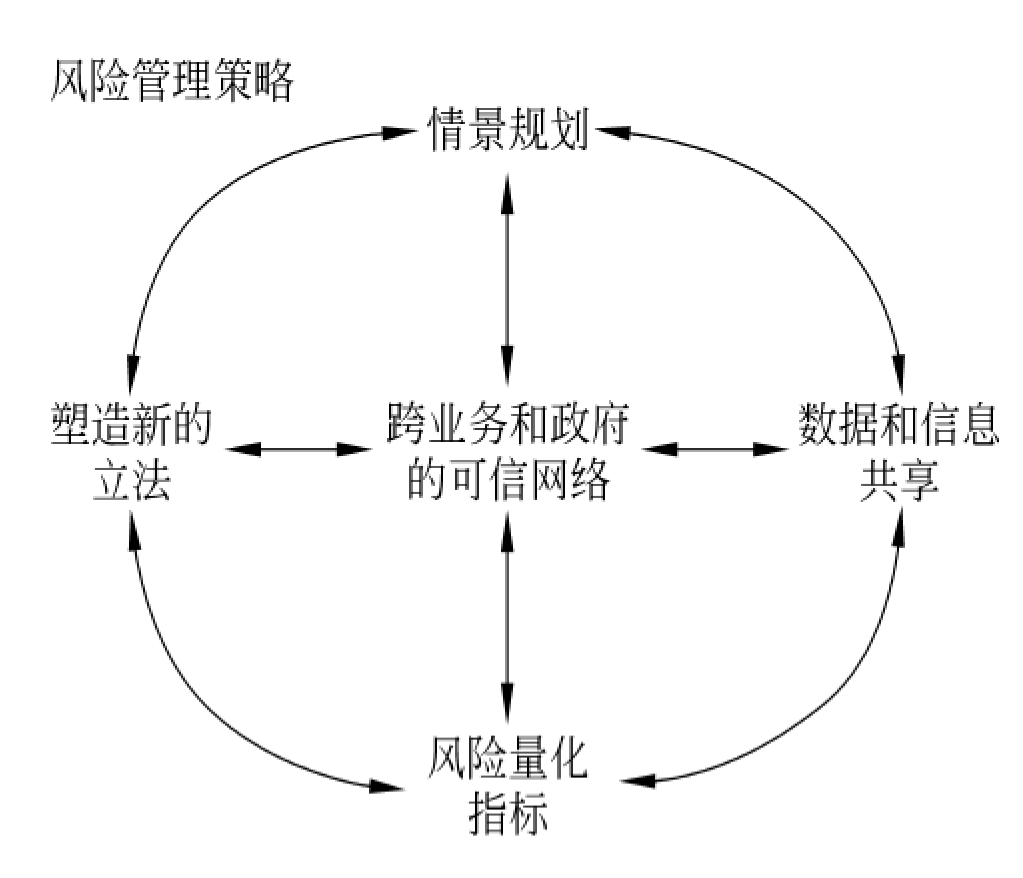


图 4-23　风险管理措施集合［WEF2012 P15］



地区范围的更大程度的理解和协调是有可能的，例如供应链风险领导委员会是由制造业和服务业供应链公司合力开发和共享的供应链风险管理的最佳案例。

达沃斯论坛在2011年建立了风险应对网络(RRN)，它接入高水平的领域专家组进行风险分析和改善风险降低工具，提高供应链和运输弹性，从而支持了可信网络的开发。服务于联合国共同物流集的物流紧急救援队伍是公司联合政府来降低供应链风险和提高响应水平的实际例子。他们认识到了在应对人道主义灾难中先进的价值评估、准备和关系建立的价值。物流紧急队伍现在被联合国视为备用的合作伙伴已经在全世界范围内部署。

2）建立相应的法律法规[WEF2012]

简化、在国际上协调和实施有效的立法是整个行业团体的关键问题。对现代工业实践的调整和规范对改进风险管理是至关重要的。然而，针对性不强的法律法规无意中加剧了对供应链和运输网络的破坏。进行风险评估和跨公司情景辅导将使决策者和业界提前确定网络漏洞，在新法律法规的设计阶段进行协商。监管机构和企业之间的进一步合作用来解决实施立法和管理的不可避免的挑战和优化目标福利。

2010年当冰岛的埃亚菲亚德拉火山喷发时，欧洲交通部门被动应对，民用航空主管部门延误了空中交通的重启。没有提前意识到冰岛火山灰带来的威胁，现有航空协议的不稳定性以及火山灰水平上缺少一致协议导致了这次供应链风险管理上的重大失误。格里姆火山在2011年喷发的时候，应急计划已经建立并为平衡安全空域的潜在影响上提供了建议。

3）进行数据和信息共享[WEF2012]

获取准确和可信的信息可以得到清晰的全球供应链网点漏洞并有助于中断事件中后备计划的协调。识别工业水平的复发风险可以帮助企业和政府致力于增加网络弹性。增强企业和政府间信息的双向流动被认为是一个特定的优先级，专家组提出了两个具体的行动建议：通过关键基础设施建立可信的宏观流和中断的仪表板；增加端到端网络的信息流以提高供应链所有层次的透明度。

目前，只有有限的工具和软件支持广泛的数据和信息共享。麻省理工学院运输和物流工程系教授Yossi Sheffi称“有一种正在开发的新型软件产品可以被公司内部和软件公司用来应对供应链风险。”这些产品旨在识别高概率和高影响的风险并对这类中断组织应对行动。

4）进行指标的量化[WEF2012]

论坛参与者认识到了能够量化和测量供应链和运输网络风险的重要性。缺少指标使一些公司难以量化自己组织的风险敞口或者难以对比供应商。开发一个公认的供应链和运输风险量化指标可以使企业和政府获得对网络风险的精确理解，更好地进行优先风险管理活动，并实现激励及风险偏好的一致化。只要有可能，风险指标在组织内部以及跨组织间应该是一致的。

5）进行情景规划[WEF2012]

情景规划目前正有效应用于操作级别上，并可能在降低跨网路系统风险上扮演不可或缺的角色。定期进行情景规划可以确保外部风险和网络漏洞不断被检测到并且

确保相关的减弱控制可以有效更新。向多方参与的级别缩放场景计划提升了对外部环境的理解同时也有助于网络伙伴更好地参与其中并造就了改进的连续性计划的联合准备。地区和/或部门级别的情景计划可以确认地区冲突和缺乏协调之处，明确角色和面对重大的全球紊乱时公共和私人部门的职责，从而提高响应的速度和有效性。对关键基础设施的强度测试将使更多的公共和私人部门理解发生中断事件时基础结构的弹性。

ABB(Asea Brown Boveri，一家瑞士-瑞典的跨国公司，专长于重电机、能源、自动化等领域)的企业风险管理过程以自底向上的方式(从国家和业务单位)和自顶向下的方式(从总部，部门和地区)收集了风险输入。经过相对可能性和影响的评估和分析，顶级风险在集团层面被确认。2010 年，这个过程使 ABB 能够识别关于日本地震和埃及政治动荡。

以上讨论的可信网络可以增加情景规划的范围和有效性，驱动应急解决方案中有效的风险管理和投资，并有助于主动塑造全球立法和监管。这些改进的风险管理的优先事项需要公共和私人部门的共同合作。新加坡经济发展董事会物流和专业服务执行董事 Kelvin Wong 认为"关键是政府和企业要合作来理解供应链和运输网络的风险，开发新的解决方案和风险管理的最佳实践。组织有机会增加全球网络的弹性，公共和私人部门的参与者必须向新的供应链风险管理模型协作迈进。"

4.6.3 模型展望

全球化运作模型的增加和供应链和运输网络的日益增长的相互联系正导致进化的风险预测和新的系统性风险管理优先级。某些外部事件对供应链和运输网络会造成广泛的、系统性的破坏。尤其需要注意的风险是信息/通信破坏和基础设施失败。进行以上工作的目标不是预测适合什么，而是准备好而且能够用已知的和计划好的方式来最小化中断的影响。供应链和运输网络以及商业模型的演变已经导致了风险分布的变化。需要考虑到供应链失败对一个组织性能和声誉的影响，对关键供应链仅仅看一级供应商已经不够满足供应链安全需求。供应链和运输网络的脆弱性可以放大中断的影响。缺乏对风险的可见性和量化将会阻碍供应链和运输网络的有效风险管理。中断可以造成超越企业财务的显著影响[WEF2012]。

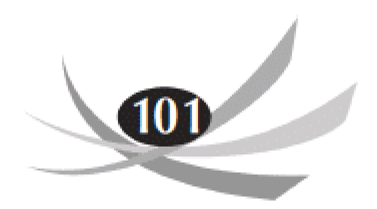
论坛专家组强调政府和企业间显著的交互需求将促使已确认的风险管理方法的提升。以下是被提议的建立解决供应链和运输风险的新模型的可能步骤：区域贸易部门领导的工作小组以区域性轴心起驱动作用；中断级别评估框架在供应链网络中断影响的标准划分上达成一致，在事件期间和之后将通知公共和私人部门进行响应；国家风险响应成熟度评估作为贸易和旅游开放性排名的一部分。

系统的供应链和运输风险通过多方行动和合作可以被更加有效地管理。关键成员是供应链和运输工业本身，以及它的客户和政府。对企业和政府解决系统的供应链和运输风险有五条确定性建议[WEF2012]：

(1) 提高国际和跨部门的弹性标准和项目的兼容性。

(2) 更精确地评估作为采购、管理和治理过程的一部分的供应链和运输风险。

(3) 发展可信的供应商、顾客、竞争对手和关注风险管理的政府网络。



(4) 通过双向信息共享和标准化的风险评估以及量化工具的合作开发,改善网络风险可见性。

(5) 改善系统破坏和平衡安全之间的交流,从而促进更加平衡的公共和私营部门的讨论。

4.7　ICT 供应链风险管理集群框架

在美国总统的《国家网络安全综合计划》(CNCI)的倡议下,美国国家标准技术协会(NIST)为了支持ICT领域的供应链风险管理的发展,负责联邦的相关政策的制定。为了支持NIST的工作,马里兰大学的斯密斯商学院在2011年8月着手开展相关调查和研究,将已有的行业和公共部门的措施应用到不同的ICT段(软件、硬件、网络和系统集成服务)。在该项目的第二个研究报告中形成了一个ICT供应链风险管理集群框架,能够将在单个风险框架中定义的不同进程和实例结合起来。这个框架包括三层:企业风险管理、系统集成和运作。这个框架提供了两个功能:深度防御和广度防御。它能够使管理者更清晰地看到框架中的每个措施在ICT风险管理生态系统中的相对位置,强调了措施的互补,促进了ICT风险管理范围内的风险识别和评估。

4.7.1　集群框架的构建基础

由于没有大规模端到端的可以跨ICT供应链各个功能区的风险管理模型存在,分别涵盖软件、硬件、电信网络和系统集成功能的行业组织只是有各自的专业知识,因此需要从概念上对各个领域专业知识进行整合,确定供应链的传递/相互依赖性,使风险治理层覆盖整个端到端过程[MARYLAND2]。

该项目中研究人员提出创建一个全面的综合框架的三个关键源:ICT供应链安全确保模型——由斯密斯供应链管理中心和SAIC经三年开发出来的有三个环的嵌套模型:内部治理环、系统集成环和行动环;供应链运作参考模型(SCOR)——由供应链委员会在1996年创造的工业参考模型,定义了一套企业风险管理活动和流程层任务,包括供应链的计划、获取、制造、交付、返回;NIST系统开发生命周期模型——将安全纳入每个阶段,从采购到处理。这个整体方法支持风险管理方法并提供全面的技术审计控制[MARYLAND2]。

利用这三个关键源可以创建一个集群框架:将这些关键元素纳入到一个拥有企业风险治理层、系统集成层和操作层的ICT三层风险管理框架,这个框架包括两大功能:广度防御和深度防御。广度防御是广泛的:它覆盖整个客户/收购者、集成商、供应商和他们之间关键过程的端到端的生态系统。深度防御是集中的:它覆盖风险治理并包括设计、风险评估和供应基地建模/审计的系统生命周期管理以及运营管理。这两个功能提供了综合的ICT供应链风险管理控制。

4.7.2 集群框架的构建

通过对200个大小不同的ICT供应商的深入调查得出结论:“网络供应链守则目前处于初期出现的阶段,可以被描述为缺乏根据的知识体系,行业最佳惯例和通常被大公司带领的标准团体的核扩散和碎片,ICT供应商的供应链连锁风险治理机制的意义深远的应用。”行业的不成熟是NIST研究项目的主题——“建立网络供应链守则(2011)”。这种不成熟在以下战略定位图(如图4-24)中得以反应,该图是通过对市场上主要措施的政策和实践文件的调查以及专家小组的建议得出的[MARYLAND2]。

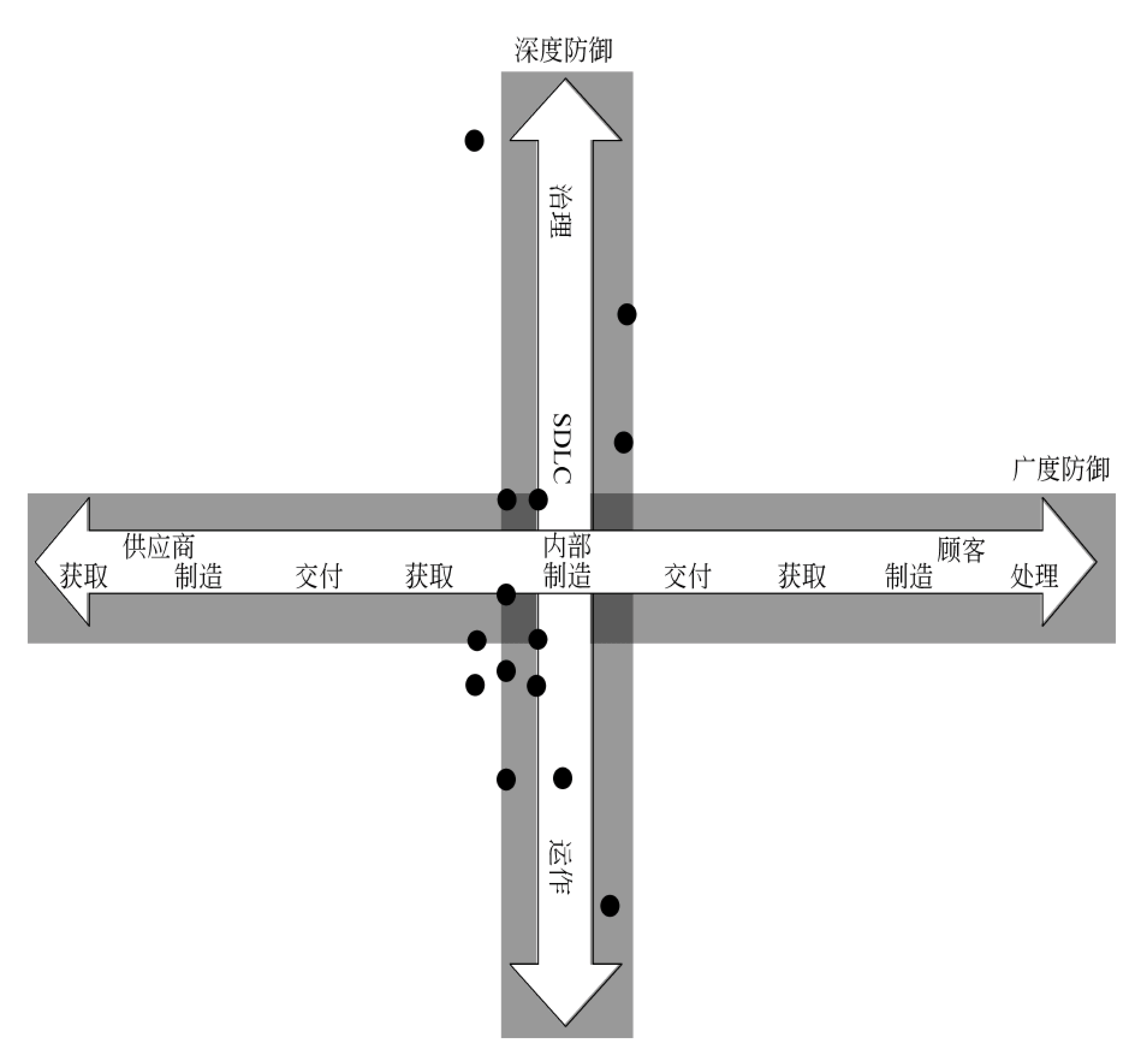


图4-24 战略定位图[MARYLAND2 P11]

图4-25代表一个进化的生态系统的静态快照,它显示了内向型系统开发和面向供应商采购功能的深度和广度防御的现有措施的聚类。我们可以看到在深度防御轴上的活动频谱的高端,风险治理似乎存在广泛的差距。事实上,位于组织最高行政级别的企业风险管理不被大多数ICT供应链风险管理组织、措施和行业惯例所强调。横跨整个供应链从而协调足够的广度防御的企业风险管理功能明显缺乏。这种缺乏首先在NIST的ICT供应链风险管理供应商调查中被确认:“在风险管理的战略层面,47.6%的抽样公司从来不使用风险委员会或者其他行政机制来管理风险;46.1%从来不使用共享的风险注册,一致的ICT供应链的在线数据库;49.4%从来不使用集成的IT供应链风险管理仪表板;44.9%从来不使用供应链风险管理计划。”

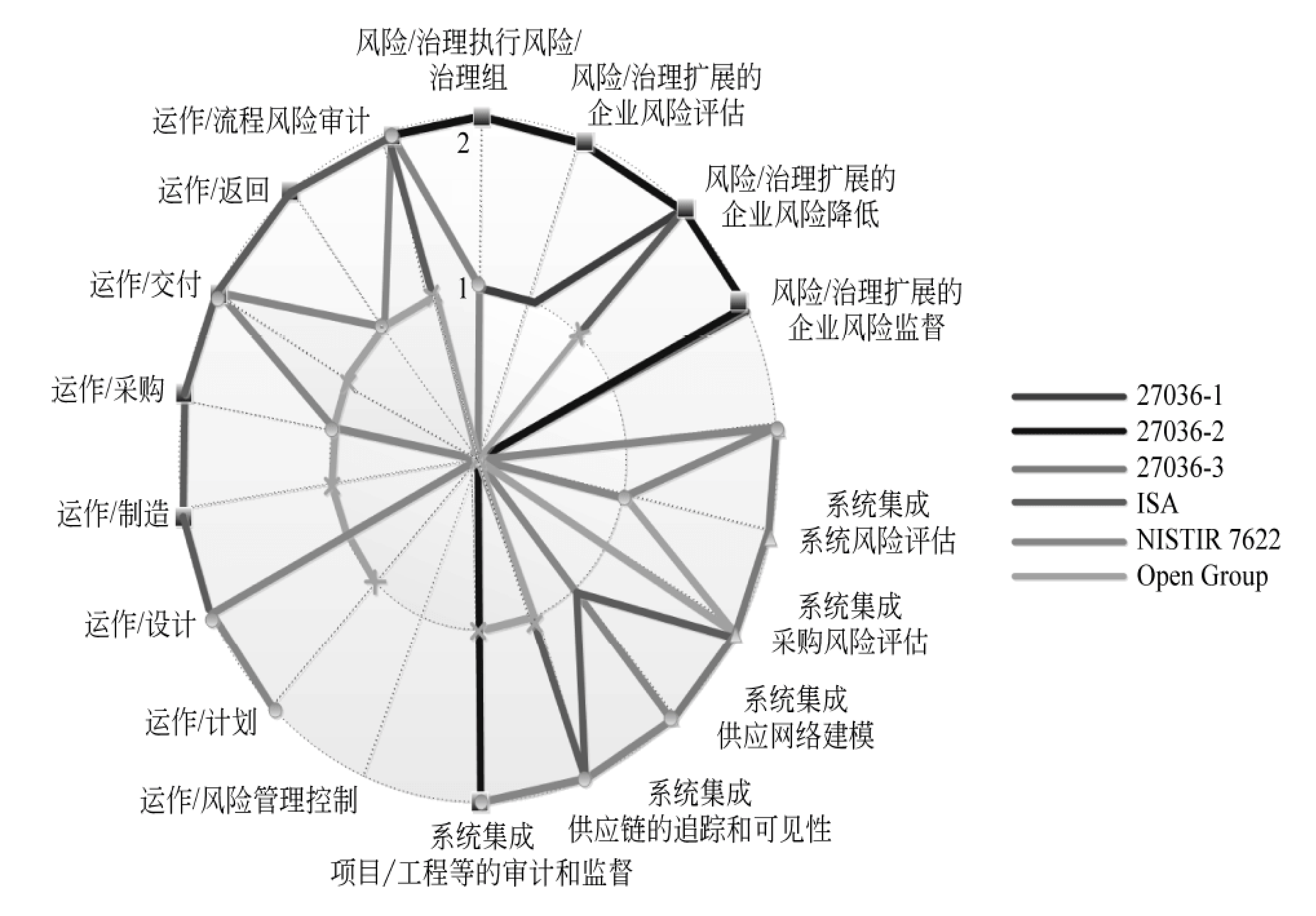


图 4-25　ICT 风险管理措施[MARYLAND2 P17]

研究项目的参与者大体上同意以上战略定位图的发现,同时也表达了他们自己组织解决这些差距的愿望并号召使用更加敏感和动态的方法来衡量新兴的组织能力。雷达图(图 4-25)代表覆盖了五个 ICT 风险管理措施(包括 Open Group,ISA 和三个主要的 ISO ICT 供应链风险管理标准开发措施)的重叠范围。

最后,通过对参与者提供的信息进行总结列出了相关机构的风险管理实践(如表 4-14)。

表 4-14　相关机构的风险管理实践[MARYLAND2 P69]

文件出处-名称	框架/属性/解决	风险管理实践
SAFeCode-安全软件开发的基本实例	系统风险评估/威胁模型化	威胁模型
	制造	使用最小特权 使用沙盒 安全编码实践:减少不安全字符串和缓冲功能的使用,验证输入和输出以减少常见漏洞,使用健壮的集成操作来实现动态内存分配和数组偏移,使用反跨站脚本(xss)库,使用规范的数据格式,避免字符串拼接来实现动态 sol 语句,消除脆弱的加密,使用日志和跟踪 测试建议:确定攻击表面,使用适当的测试工具,执行模糊/健壮性测试,执行渗透测试

续表

文件出处-名称	框架/属性/解决	风险管理实践
SAFeCode-软件集成控制	系统风险评估/威胁模型化	供应商的供应商应该：在设计、开发和测试阶段处理安全威胁，确保创建和传送产品的过程是安全的，确保提供区分真假的方法 供应商应该与以下供应商有书面协议：定义预期，定义知识产权所有权和保护代码的责任，理解供应商漏洞并定义应对程序 开放源码软件：实现更积极的漏洞管理和突发事件的处理，开发可以验证开放源代码软件安全性的方法 对供应商的技术完整性控制 安全的传输：经过身份验证的端点，加密的传输，端到端进程的自动化 系统和网络资源的共享：数字认证技术提供有限的访问权，对每种资源按照授权要求进行独立评估，供应商的访问应在项目结束前结束 对供应商的技术完整性控制： 恶意软件扫描：使用最新的恶意扫描软件 安全存储：代码应使用须知访问控制储存，代码包应迅速转移到安全的存储库中 源代码交换平台：使用数字签名方案和可核实的校验或散列，用经过验证的时间戳验证数字签名
	制造	人员安全：职责划分，使用控制的自动化流程，清楚地定义角色、职责和访问权限，管理者应知道谁有访问权，进行安全开发和安全技术控制训练 物理安全：使用访问控制，安全性应定期重新评估 网络安全：网络安全应该使用基于风险的进程；包括源代码在内的会话交通应该加密到可接受的标准；访问开发人员工作站应该受到控制；离职人员的账户应该立即禁用；工作站和虚拟机应预防恶意代码的插入；开发者应该有权力访问保证完成任务的最小代码 代码库安全：所有代码相关的资产应该存储在源代码存储库用于安全和访问控制；托管源代码的服务器应该安全地封装；当在不同的数据库存储时应保持代码的机密性；系统在默认状态是安全的；默认的安全配置状态应该被保护；通过公司身份系统来控制对源代码存储库的访问；对所有代码修改记录日志；维护和管理所有产品的代码资产的清单 构建环境安全：构建环境应该尽可能的自动化；应该具有构建脚本的行为高可跟踪性；建立自动化脚本，它们的变化应该在源代码库与制造变化的人的名字对应；服务账户 同业互查： 使用自动化工具来实现可伸缩性；将同业互查聚焦于那些再次扫描并等待批准的改变了的代码 测试安全代码：测试工具——静态代码分析工具（源代码）；网络和 Web 应用程序漏洞扫描仪（动态测试）；二进制代码分析工具；恶意软件检测工具（发现后门等）；安全合规验证工具（硬化、数据保护）；代码覆盖工具

续表

文件出处-名称	框架/属性/解决	风险管理实践
SAFeCode-软件集成控制	交付、收回	恶意软件扫描; 代码签名; 交付; 转移; 加密散列或数字签名组件; 通知技术; 在程序执行时的真实验证;修补; 安全配置; 定制代码扩展
卡内基梅隆-软件供应链风险管理:从产品到系统的系统	系统生存期集成/风险设计	系统开发和集成承包商应该能够:分析和商业产品相关的软件风险;管理与比期望的确保水平低的组件的集成相关的风险;保持员工具有软件弱点和减排的大量知识;按照系统威胁模型引导的那样测试应用系统开发和集成的弱点
	系统风险评估/威胁模型	攻击分析:攻击的推动者;攻击面;攻击目的;风险因素;
	收购风险评估/采购管理	供应商:减少缺陷:(1)威胁模型:分析风险,在开发过程中确定安全模型的系统化方法,包括详细的流量分析;(2)测试:渗透测试,模糊测试-测试畸形的数据输入 减少攻击目标:攻击表面分析:注意并处理风险,隔离的分区代码风险 供应商选择:(1)选择意识到风险存在并采取措施缓解的供应商(2)供应商风险管理认证应该寻找:开发人员在可开发的软件缺点和缓解缺点上是知识丰富的,物理、人员和工业安全措施,开发设施强大的配置管理,对员工的仔细审查,评估和检测自己的供应商和分包商
卡内基梅隆-评估和减轻软件供应链安全风险	收购风险评估/采购管理	使用攻击面分析:进行一个初始的供应链安全评估;供应链安全风险管理作为意见书的一部分;供应链安全风险管理监测案例;评估交付的产品/系统;考虑供应链安全风险的配置/集成;开发用户指南来帮助缓解供应链安全风险
		使用风险评估(威胁模型):编写建议书的软件供应链安全风险管理部分;选择重视供应链安全风险的供应商;监控供应链风险管理实践;评估交付的产品/系统;考虑供应链安全风险的配置/集成;监控组件/供应商
	收购风险评估/采购管理	供应商安全属性已经到位的证明:架构和设计分析;开发编码的实例信息;存在提供攻击表面分析和减缓计划的建议书的需求;在验收测试中加入安全测试的计划;安全测试的结果

续表

文件出处-名称	框架/属性/解决	风险管理实践
国土安全部门-安全软件的架构和设计考虑	系统生存期集成/风险设计	软件设计产品：模型、原型和模拟以及它们的相关文档，初步用户手册，初步测试需求，文档可行性，结构设计需求的可追溯性文档
		抽象：通过消除不必要的细节和隔离最重要的元素来使设计更加易于管理的用于降低系统复杂性的进程
		分解：描述抽象概括的进程
		减少后果严重的目标的数量：最少特权原则，特权、关税和角色的分离，领域的分离
		不要暴露易受攻击的或者后果严重的组件：保持程序数据、可执行文件和配置数据是分离的，从不可信实体中隔离出可信实体，最小化入口和出口点的数量，假定环境数据是不可信赖的，只使用环境资源的可信接口
		否认攻击者意味着妥协：简化设计，保存所有可计算的角色，定时、同步和测序应该简化为避免问题，使安全状态容易，易受攻击的状态难以进入，可控性设计，全失败设计
		机制经济：保持设计尽可能简单
		故障保险违约：基本的访问权限而不是排斥
		完整的中介：访问每个目标都必须检查授权
		开放设计：设计不是秘密
		特权分离：需要两个密钥的保护机制比只需要一个密钥就允许访问的更健壮和灵活
		最小特权：系统的每个程序和每个用户应该使用完成工作所需的最小特权集
		最少的公共机制：最小化对多个用户公开的并被使用的机制数量
		心理上可接受性：与人的接口应该便于使用以使人们正确的应用保护机制
		安全设计模式：不可信的分解，特权分解，听从受限制的应用或区域
		设计水平模式：安全状态机制，安全的访问者
		安全性和保险性的多个级别：数据分离，信息流，卫生处理，损害限制
	系统风险评估/威胁模型	威胁模型：分解：通过人工检验来理解应用程序如何工作，包括它的资产、功能和连接；定义和分类资产：分为有形资产和无形资产并按照商业影响排序；探索潜在漏洞：技术的、操作的或者管理的；探索潜在的威胁：使用威胁或者攻击树从攻击者的角度探索潜在攻击的现实视野；创建减缓策略：为每一个可能成为现实的威胁开发缓解控制

续表

文件出处-名称	框架/属性/解决	风险管理实践
国土安全部门-安全编码	计划,设计	准备编写安全代码:选择一种有安全意识的语言,创建一个安全的开发环境,创建一个应用程序指南,确定安全可靠的软件库
	制造	安全编码原则:保持代码小而简单,使代码前后都可追踪,用于重用和可维护的代码,遵守安全的编码标准和/或指南,使用编译器安全检查和执行,避免本地和非本地,主动和被动代码之间的安全冲突,编码和编码之后的评审代码
		安全编码案例:SANS 前 25 错误列表/OWASP 前 10 列表,验证和编码输入,过滤和净化输出和调用,减少状态信息的保留,不允许未经授权的特权升级,经由模糊的杠杆安全只是一个附加的威慑措施,合并进程间身份验证,杠杆攻击模式,实现加密和散列,在部署之前禁用调试工具
		安全的记忆和缓存管理:限制持久的内存缓存,仔细分配内存和其他资源
		安全的错误和异常处理:集成异常意识,合并运行时错误检查和安全执行,使用事件监视器
国土安全部门-安全软件需求和分析	系统风险评估/安全模型化	诱发安全需求:滥用案例,威胁分析,软件系统方法论,质量功能展开,控制需求表达,基于信息系统的问题,联合应用程序开发,面向特征的领域分析,批评话语分析,加速需求方法
		安全需求开发的方法:全面的轻量级的应用程序安全过程,安全品质需求工程,核心安全需求工件
		需求排序方法:二叉查找树,数字分配技术,计划博弈,100-逐点计算法,W 理论,需求分类,韦格方法,层次分析法,需求优先级框架
国土安全部门-减轻最严重的可开发软件缺陷的关键案例	计划,设计	需求,架构和设计阶段,以下方面的预防和缓解案例:不适当的输入验证,不适当的编码或转义输出,无法保存 SQL 查询结构,无法保存 Web 页面结构,无法保存 OS 命令机构,敏感信息的明文传输,跨站点请求伪造,竞态条件,不能约束内存缓冲区边界的操作,对临界状态数据的外部控制,对文件名或者路径的外部控制
		以下方面的预防和缓解案例:(续):不可信的搜索路径,不能控制代码的生成,下载未经完整性检查的代码,不适当资源的关闭或释放,不适当的初始化,不适当的访问控制,使用已经被破解或者高风险的加密算法,硬编码密码,关键资源的不安全许可分配,不够随机的值的使用,在不必要的特权下执行,服务器端安全的客户端执行

续表

文件出处-名称	框架/属性/解决	风险管理实践
国土安全部门-减轻最严重的可开发软件缺陷的关键案例	制造	构建、编译、执行、测试和文档，对以下方面的预防和缓解：不适当的输入验证，不适当的编码或转义输出，无法保存 SQL 查询结构，无法保存 Web 页面结构，无法保存 OS 命令机构，敏感信息的明文传输，跨站点请求伪造，竞态条件，错误消息信息泄露，服务器端安全的客户端执行，不能约束内存缓冲区边界的操作
		预防和缓解案例（续）：关键状态数据的外部控制，文件名和路径的外部控制，不可信的搜索路径，不能控制代码的生成，下载未经完整性检查的代码，不适当资源的关闭或释放，不适当的初始化，不正确的计算，使用已经被破解或者高风险的加密算法，不合适的访问控制，关键资源的不安全许可分配，不够随机的值的使用，硬编码密码，在不必要的特权下执行
		安装、操作和系统配置阶段，预防和缓解措施：无法保存 SQL 查询结构，无法保存 Web 页面结构，无法保存 OS 命令机构，关键状态数据的外部控制，敏感信息的明文传输，错误消息信息泄露，不能约束内存缓冲区边界的操作，文件名或路径的外部控制，不能控制代码生成，不适当的访问控制，关键资源的不安全访问许可
国土安全部门-软件供应链风险管理和严格评估	项目风险评估/监督	软件确保关注类型：软件历史和许可，开发过程管理，软件安全训练和意识，计划和需求，构建与设计，软件开发，嵌入软件防护，组件装配
		软件确保关注类型（续）：测试，软件制造和包装，安装，保险索赔证据，支持，软件变化管理，脆弱性缓解的时间性，个人恶意行为，安全“跟踪记录”，金融历史和现状，组织历史，外国利益和影响，服务保密政策，用于服务的操作环境，安全服务和监测

4.7.3 框架展望

随着 ICT 供应链风险管理行业的成熟，人们会逐渐形成措施上的共识。ICT 供应链风险管理集群框架通过映射寻求改善保护网络供应链的主要举措。每个举措有各自处理问题的角度，在深度防御和广度防御中存在一致性，如表 4-15 所示。

物供应链在 20 世纪 90 年代实现了全球化。如今，ICT 供应链面临巨大的挑战：需要跨越硬件、软件、网络和物理分布以获得更大的战略指挥和控制；需要更好地利用从其他供应链规则中学到的经验；需要更有效地处理与 ICT 系统的迅速全球化有关的机遇和风险。我们下一步的任务是创建一个可以围绕生存和生长的共同核心集体，从而促使 ICT 供应链风险管理更加成熟[MARYLAND2]。

表 4-15 深度防御和广度防御中措施的一致性列表[MARYLAND2 P19]

供应链风险管理措施的共识领域					
	属性|措施	Open Group	ISA	ISO 27036	NIST
关键实践	持续评估和优化实践	×		×	×
	对实践形成文档并实施标准化	×	×	×	×
	供应商绩效评估积分卡	×		×	×
进程	统一的验证过程	×	×		×
	威胁建模	×	×		
	风险评估	×		×	×
	脆弱性分析 & 响应	×	×	×	×
	产品开发 & 审计进程				×
	风险缓解选项		×	×	×
技术	定义的安全编码标准	×		×	
	物理安全访问控制	×			×
	自动化/文档资产	×			
	信息系统分类		×		×

参考文献

[BSSDLC] James E. Purcell. Building Security into the System Development Life Cycle (SDLC): A Case Study.

[MARYLAND2] University of Maryland. The ICT SCRM Community Framework Development Project. Final Report.

[LHH2009] 刘浩华.供应链风险管理.中国物资出版社.2009.

[NIST2008] National Institute of Standdards and Technology. Security Considerations in the Information System Development Life Cycle- information security. 2008.

[OnPoint] OnPoint. Incorporating Security into the System Development Life Cycle(SDLC).

[SCC2005] Supply-Chain Council. Supply-Chain Operations Reference-model, SCOR Version 7.0 Overview. 2005.

[SAIC&SCMC2009] SAIC and SCMC. Building A Cyber Supply Chain Assurance Reference Model. 2009.

[TLSSC2011] Price Waterhouse Coopers (PWC). Transportation & Logistics 2030 Volume 4: Securing the supply chain. 2011.

[WEF2012] World Economic Forum. New Models for Addressing Supply Chain and Transport Risk. 2012.

[WZ1] http://www.docin.com/p-599291246.html.

[WZ2] http://wenku.baidu.com/link? url=qmBlgtZT9zrs86Js3DnJ8CFo1kM7kt1nVpm0EWs9pQfAt-5yfjj9xHH8T41puJnQQ81lIbEXTvl3A8XcR1QgybkMa0uqRxqMDZ8rIkiHS3bm.

[WZ3] http://www.docin.com/p-110173805.html.

第5章 ICT 供应链安全标准

5.1 概 述

ICT 供应链中的软件供应链安全、硬件供应链安全、采办安全以及外包安全,涉及到了供应链中的采购商、供应商、外包商等关键角色的活动,而这种活动必须由相关统一的标准来进行规范。标准的存在与利用使产品和服务的生产、销售与购买更加便利,是推动经济增长和技术创新的“经济基础设施”的一个必要组成部分。本章将介绍国际上影响力较大的与 ICT 领域相关的供应链安全标准,它们分别是 ISO① 28000(供应链安全管理体系规范)、ISO 27036(ICT 信息安全标准)、ISO 15026(系统与软件确保标准)和 NIST IR 7622(网络供应链风险管理指南)。

5.1.1 对标准的理解

标准产生于人类社会的生产和交换活动。产业革命后,各种标准更成为货币经济运行的必备要件和“基础设施”。早期的标准基本是作为“公共产品”出现,不包含有任何私有产权的。早期的通信产业标准大多也是以“公共标准”的面目出现的,其目的是维护通信网络的互联互通。但随着信息技术与通信技术的融合,传统上以“私有标准”开始渗入通信领域,并通过市场竞争成为 ICT 产业的事实标准,并对 ICT 产业的发展产生了重要影响[ZT2005]。标准实际上是思想与知识的一种存在形式,是社会发展一定阶段所积累的公共知识的载体,在经济中发挥着日益重要的影响。从对经济活动的直接影响看,标准的经济功能主要表现在四个方面,但由于各类标准的使用范围和作用方式不同,并不是每一类标准都具有所有 4 种功能[ZT2006]。

(1) 降低交易成本。有了公认的质量标准,不仅可以降低产品购买者的风险,而且可以减少购买者在购买前用于评价该产品所花的时间和精力。很难想象,不存在一个明确界定的标准等级,以及鉴定所交易的产品符合该等级的标准情况下,能够进行大规模的贸易活动。

(2) 缓解交易双方信息不对称。如果没有反映产品属性的质量标准,消费者在交易之前就无法了解并评价产品质量。而质量标准有信号显示效应:遵守一种质量标准的产品可以通过显示满足产品的最低要求的信息来降低买卖双方的信息不对称,帮助消费者

---

① ISO,即国际标准化组织,1947 年成立于英国。目前总部在瑞士日内瓦,其宗旨是在全世界促进标准化及有关活动的发展,以便于国际物资交流和服务,并扩大知识、科学、技术和经济领域中的合作。

正确的识别产品质量的高低，从而减少逆向选择造成的市场失败[ZT2006]。

(3) 减少产品种类，实现规模经济。标准限制了产品特征的数量和特定范围，如产品规格或质量水平，从而限制了消费者的选择范围。但在产品种类下降的同时，扩大了每一类产品所能获得的市场规模，有利于实现生产的规模经济。随着ICT的发展，产品种类的减少不再只是一个选择产品标准化的物理尺寸问题，产品种类的减少也反应在数据库格式等非物理属性，以及结合了物理与功能属性的界面方面[ZT2006]。

(4) 确保产品兼容性。兼容标准可以起到扩大兼容产品的市场规模的作用。比如一种原来只能在一种汽车上使用的零件现在可以用于所有汽车。在ICT产业，兼容标准的一个更为重要的市场后果是启动了不同技术或产品用户之间的网络效应。这是ICT产业的兼容标准引起众多经济学家关注的主要原因[ZT2006]。

5.1.2　ICT供应链相关国际标准

ICT供应链安全是近年来凸显的新问题，目前还缺少成熟的ICT供应链安全风险管理标准。与此相关的已有标准分为三类：第一类是传统供应链安全管理国际标准；第二类是供应链信息安全国际标准；第三类是供应链系统安全国际标准。

1. ISO 28000 供应链安全管理体系

ISO国际标准化组织针对人类、货物、基础设施和设备(包括传送方法)等方面的安全事故，制订了ISO 28000供应链安全管理体系系列文件，以预防供应链中可能出现的破坏性影响。ISO 28000的出发点是满足运输和物流行业对共同安全管理标准的需求，最终目标是改进供应链的全面安全。它提出的通用方法可用于IT供应链安全风险管理工作，但其目的是为了应对运输和物流领域的典型威胁，尚不足以处置ICT环境中的所有威胁场景[ZL2012]。

2. ISO/IEC 27036 信息安全管理标准

ISO/IEC 27036《IT安全　安全技术　供应商关系的信息安全》是国际标准化组织(ISO)与国际电工委员会(IEC)针对供应链领域的特点专门制定的信息安全管理国际标准，是ISO/IEC 27000信息安全管理标准体系的组成部分，为定义、实施、操作、监控、评审、保持和改进供应商关系管理规定了通用性的信息安全要求。这些要求覆盖了外包、产品和服务采购等各类情况，例如制造业或装配业、业务过程采购、知识过程采购和云计算服务，普遍适用于所有类型、规模和性质的组织。其最初的出发点不是为了管理和控制ICT供应链的安全风险，但在美国标准化专家的努力下，目前ISO/IEC 27036已经为ICT供应链安全制定了子标准，即ISO/IEC 27036-3 ICT信息安全风险管理。

3. ISO/IEC 15026 系统和软件确保标准

大规模的系统代表复杂的供应链整合，这些系统来自多个供应商，这些供应商雇佣世界各地的人们，大多数系统依靠软件实现它们的大部分功能。在软件和系统确保以及其他密切相关的领域，许多专业和附属专业使用不同的词汇来表示相同的概念。为了应对软件和系统的缺口风险，国际标准化组织(ISO)与国际电工委员会(IEC)联合出台了

15026 国际标准[①],旨在提供一个可以使不同的学科可以联系到一起的总体框架,与现有的生命周期进程标准相联系。

为了帮助那些必须应对来自全球供应商以及有潜在威胁的企业和机构合理规划和管理信息采购、系统开发、系统或系统间运营中遇到的各种问题,并在控制成本、严格执行计划及满足开发需求方面有所改进,美国国家标准与技术研究院(NIST)草拟了一套做法 NISTIR 7622,旨在购买、开发和运营过程中消除高影响联合信息系统面临的生命周期供应链风险。NISTIR 7622 阐释了供应链风险管理在 ICT 领域的应用,提供了一套可直接应用于那些级别达到 FIPS(Federal Information Processing Standards,联邦信息处理标准)标准的采购与合同实例。

5.2 ISO 28000

ISO 28000 是国际标准化组织(ISO)起草制定的供应链安全管理体系规范的技术编号。ISO 28000:2005《供应链安全管理体系规范》是该系列第一项发布的标准。作为新的管理体系规范,它首次为操作或依赖供应链中某一环节的组织提供了有关框架,帮助行业各部门审核安全风险并实施风险管理措施来管理供应链中潜在的安全威胁和影响其管理方式与其他基本业务原则如质量、安全和客户满意度的管理方式相同。ISO 28000:2007 是对 ISO 28000:2005 的修订和替代,于 2007 年 9 月正式获得批准,此管理体系规范考虑到了现有的海关要求,被认为是最具深远意义的解决方案[WZ1]。

为了配合 ISO 28000 的顺利执行,国际标准化组织同时制订了 ISO 28001、ISO 28003、ISO 28004 作为补充。ISO 28000 系列标准为:ISO 28000 供应链安全管理体系规范(2005/2007);ISO 28001(2007.1.18-2007.6.18)《供应链安全管理体系——供应链安全、评估和计划的最佳实践——需求和指南》,用以补充 ISO 28000 的规定要求,为组织机构做出更好的风险管理决策提供实用的指导,为独立的第三方的审核活动提供选项,以配合和补充世界海关组织的框架标准,保护和促进全球贸易;ISO 28003(2006.12.5-2007.5.7)《供应链安全管理体系——提供审核和认证功能的实体的需求》定义了相关组织机构进行认证实体和相关审计工作时的最大需求;ISO 28004(2006.9.1-2007.2.1)《供应链安全管理体系——ISO 28000 实施指南》,对 ISO 28000 的基本原则进行解释说明,并描述其目的、特有的输入程序、过程和特有的输出程序,旨在协助标准使用者理解和实施 ISO 28000,从而获取更大的利益。

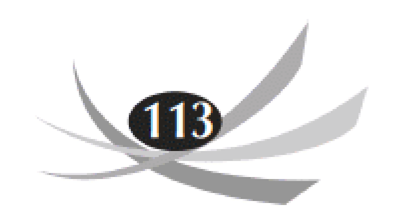
5.2.1 ISO 28000 的产生背景

在当今市场上,组织需要在多个供应商、多个供应线路和日益增加的国际要求的动态

---

① ISO 和 IEC 作为一个整体担负着制订全球协商一致的国际标准的任务,在信息技术方面 ISO 与 IEC 成立了联合技术委员会(JTC)负责制订信息技术领域中的国际标准。

IEC,即国际电工委员会,1906 年成立于英国。目前总部在瑞士日内瓦。它的宗旨是促进电气、电子工程领域中标准化及有关问题的国际合作,增进国际间的相互了解。



环境下实施管理。具有复杂供应体系的高度发展的组织认识到需要将供应链组建成一个有效的全面供应网络,从而在供应链间实现安全的贸易活动。通常来说,管理体系的基本要求能强化良好的运营能力,从而增加政府及客户的信任。强化产品保护、防止货物篡改、防止走私等措施意味着确保准时交付保质的产品,能增进客户的满意度[QSQG2006]。

2005年1月1日,有40多年历史的美国物流管理协会(Council of Logistics Management,CLM)更名为美国供应链管理专业协会(CSCMP),标志着全球物流进入供应链时代。从物流到供应链,是物流产业发展从量变到质变的必然过程。按照CSCMP的定义,供应链管理是物流管理的深度和广度的扩展,是联系企业内部和企业之间所有物流活动和所有商业活动的集成。市场竞争也从原来的企业与企业的竞争向供应链与供应链之间的竞争发展。但由于参与供应链管理的组织都是独立的法人实体,其物流、资金流、信息流以及环境等方面存在着很多薄弱环节和风险隐患,这些都威胁着供应链的安全运行。因此,供应链管理已经成为全球公认的发展方向,其强调的安全管理就是供应链管理顺利实施的保障[LH2010]。

源于自然或人为灾害的全球供应链的安全风险问题成为现今国际营商的主要挑战之一。一些具有翔实记录的事故,如地震、飓风、亚洲海啸、恐怖和犯罪活动等,突显了人们迫切需要一个系统化及其协调性的解决方案。超大规模及高价值的全球供应链,正受到日益频繁的各种形式的威胁的挑战,市场上无数的国际及区域安全法案使确保国际性的符合性变得复杂和昂贵,随着世界各国建立了各自的法案,有必要提出国际标准以包含国际市场的要求。为了提升供应链的安全性,国际标准化组织着手制订了ISO 28000系列标准[WZ1]。

5.2.2 ISO 28000的内容

1. ISO 28000:2007

《供应链安全管理体系 规范(ISO 28000:2007)》作为一套供应链安全管理规范,为组织提供了一个系统的、全面的、有序的管理模式,概述了对一个组织建立、贯彻、维持和改进供应链安全管理体系的要求。它包括对供应链的安全保障至关重要的要素,涉及到(但不限于)金融、制造、信息管理、在不同运输方式之间包装、储存、运送货物的设备以及场地等,还包括把货物从原产地运输到最终目的地的全过程,涉及到货物的流动、运送数据、相关的步骤以及一系列动态的关系[LH2010]。

它包括了许多实体,如货物的生产者、物流经营公司、组装业者、卡车运输公司、铁路运输公司、航空货物承运人、海运仓库经营者、海运承运人、货运和清关代理人、金融和信息服务部门和被运输货物的买主。当然,一个公司可以使用多个物流公司,卡车运输公司可以转包给经营者或其他公司,船舶经营公司可以把货物转移给其他承运人。它是应运输和物流行业对共同安全管理标准的需求而发展并提出的,其最终目标是保证供应链的全面安全。作为一种新的管理体系规范,它首次为操作或依赖供应链中某一环节的组织提供了管理框架,它能帮助各组织评估安全风险,通过实施控制和减轻风险的安排来管理供应链潜在的安全威胁和影响,它的管理方式与其他基本业务原则如产品质量、生产安全

和客户满意度的管理方式相同[LH2010]。

ISO 28000:2007 有以下几个特点:强调全过程控制和持续改进原则,制定包括持续改进与遵守法规的供应链安全管理方针,并将其在体系诸要素中具体化和落实,从而控制各类供应链安全管理风险,并通过体系运行的不断改进而实现绩效改进的目的;强调系统化、结构化的管理体系,实施有效的供应链安全管理,必须在物流单位内部建立由五大基本过程构成的结构化、由 19 个相互有机联系要素组成的系统化管理体系;强调最高管理者的承诺和责任及全员参与。最高管理者承诺方针,并为体系运行提供必要的组织和资源保证,是体系有效运行的前提;而体系成功实施的基础,是全体员工供应链安全管理意识的提高和各相关层次与职能人员积极的参与,并以高度责任感完成其相应的职责。强调程序化和文件化,许多要素的活动需要建立与保持程序,许多要素的活动需要形成文件[LH2010]。

ISO/DIS 28000 将供应链定义为"一组相互联系的资源和过程,以原材料的采购为起点,经各种运输方式将产品或服务交付最终用户。而供应链将包括销售商、设施制造、物流供货商、内部分销中心、分销商、批发商以及联系最终用户的其他实体"。通过运用过程方法和"计划-实施-检查-处置"的方法来应付供应链的潜在风险。ISO 28000 要求组织机构的最高管理层制订安全管理总方针,与组织机构的安全威胁和风险管理整体框架一致,并与组织机构所面临的威胁及其运作的性质和规模相称,此方针必须加以部署和实施,包括安全风险的评估和计划、有效实施和运作、检查和纠正措施及管理评审[WZ2]。

ISO 28000 标准适用于从小型到跨国公司,不论其处在产品或供应链的制造、服务、存储或运输的任何阶段,只要有建立、实施、保持和改进安全管理体系,确保与规定的安全管理方针保持一致,证实其符合性,寻找由权威的第三方认证机构对供应链安全管理体系的认证/注册的愿望并符合本标准的自我声明的组织。图 5-1 所示的 ISO 28000 标准运行过程图,阐释了安全管理体系的如下 5 个步骤。

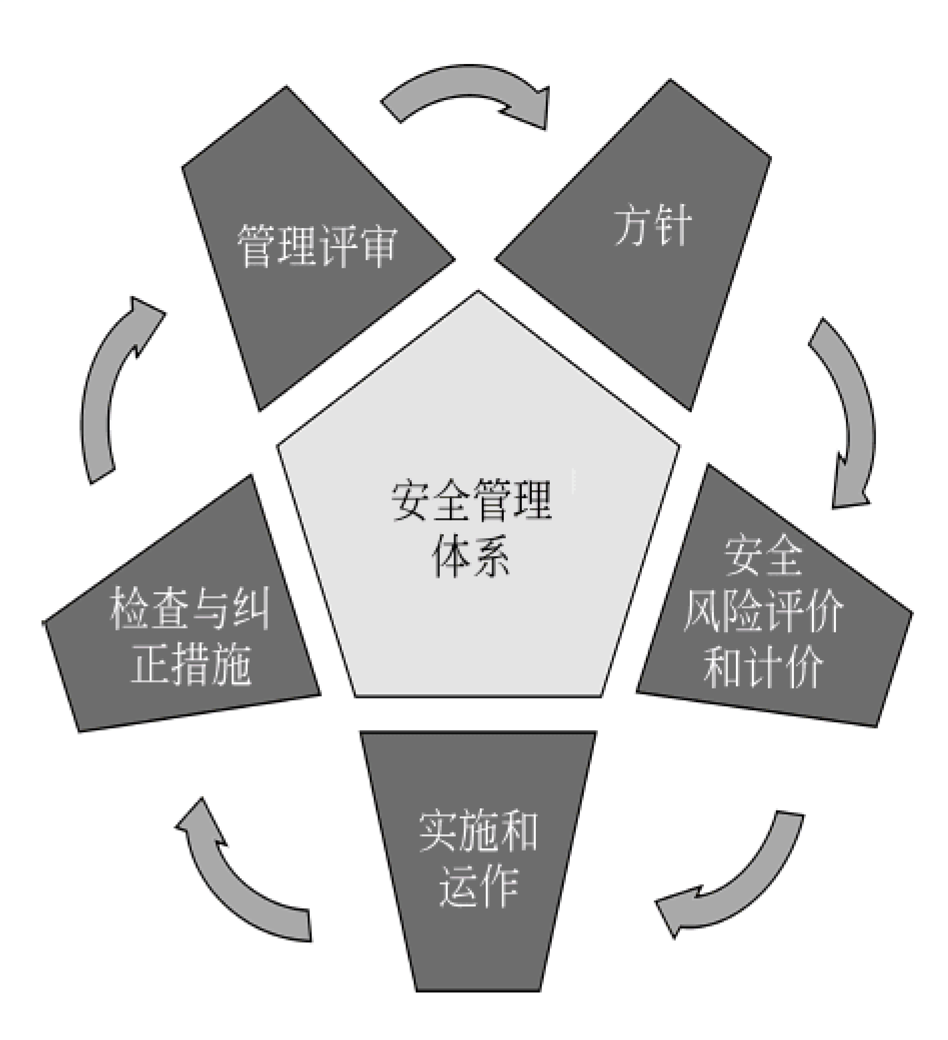
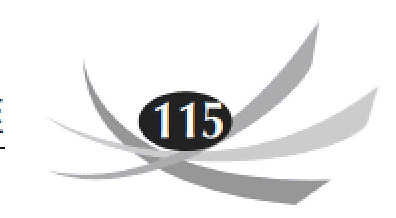


图 5-1 ISO 28000 安全管理体系的过程图[WZ1]

(1) 安全管理方针[ISO 28000]。最高管理者应制定本组织的安全管理方针,并说明为满足内部使用的需要,组织可制定一个详细的安全管理方针,该方针能为其安全管理体系(其中有一部分有机密的)的启用提供充足的信息和指导,并且还可以将包含一般目的的简述(非机密)的版本分发给其相关方和其他利益方。

(2) 安全风险评价和策划[ISO 28000]。组织应建立和保持程序,以识别和评价安全威胁和与安全管理相关的威胁与风险,识别和实施必要的管理控制措施。至少,安全威胁和风险识别、评价和控制方法应与组织的特性、运行规模相适宜,评价应考虑到某个事件及其所有后果的可能性;组织应保持信息的更新,应就符合法律和其他要求的相关信息与其雇员和其他的相关方包括合同方进行沟



通;在组织的相关职能和层次上建立、实施和保持形成文件的安全管理目标,目标应符合安全方针并与之保持一致;建立、实施和保持适合组织需要的形成文件的安全管理指标,指标应来源于安全管理目标并与之保持一致;建立、实施和保持安全管理方案,以实现其目标和指标,应优先采用合理化方案,并高效率、低成本地实施这些方案,应定期评审安全管理方案,以确保它们持续有效和与目标指标保持一致。

(3) 实施和运行[ISO 28000]。组织应建立和保持组织的职能机构、职责和权限,与其安全管理方针、目标指标和方案相一致,应对职能机构、职责和权限做出明确规定,形成文件,并就此与负有供应链安全管理体系实施和保持职责的个人进行沟通;应确保在安全设备和过程的策划、运行和管理方面负有责任的每个人具备相应的教育、培训和(或)经验;应制定程序以确保有关的安全管理信息在相关的员工、合同方和其他相关方中得到沟通,因为某些安全相关信息敏感的特性,对敏感信息应在发布之前进行充分的考虑;应建立和保持安全管理体系文件,包括但不限于安全管理方针、目标和指标等并确定安全信息的敏感性,并应采取措施防止未授权侵入;应根据标准对所有文件、数据和信息的控制建立和保持程序确保这些文件、数据和信息只能由授权人查找和访问;应识别那些必要的运行和活动并确保这些运行和活动在规定的条件下得到执行,适当时,这些程序应包括对设计、安装、运行、返工和更改与安全相关的设备、仪表等的控制;应建立、实施和保持适宜的计划和程序,以识别潜在的安全事件或紧急情况,并做出响应,以便预防和减少可能随之引发的后果。

(4) 检查和纠正措施[ISO 28000]。它要求组织设定监测和测量关键特性参数的频次,考虑相关的安全威胁和风险,包括潜在的恶化过程及其后果。应通过定期的评审、测试、事后报告、已学课程(培训实施)、绩效评估和演习来评价安全管理策划、程序和能力。这些因素中的重大变更必须及时地在程序中得到反映。定期对适用法律、法规、行业最佳实践的遵守情况及方针和目标指标的符合情况进行评价并保存对上述定期评价结果的记录。建立、实施并保持安全相关的失效、事件、不符合及纠正和预防措施的程序,在程序中规定职责和权限,这些程序应要求,对于所有拟定的纠正和预防措施,在其实施前应先通过安全威胁和风险过程进行评审,除非处在生命或公共安全的紧要关头,为消除实际和潜在的不符合而采取的任何纠正或预防措施,应与问题的严重性和面临的安全威胁和风险相适应,组织应实施并记录因纠正和预防措施而引起的对形成文件的程序的任何更改,必要时,还应包括培训的要求。根据需要,建立并保持必要的记录,用来证实对安全管理体系及本标准要求的符合,以及所实现的结果。建立、实施和保持安全管理审核方案,并应确保按照策划的时间间隔对安全管理体系进行内部审核。

(5) 管理评审[ISO 28000]。最高管理者应按计划的时间间隔,对组织的安全管理体系进行评审,以确保其持续适宜性、充分性和有效性。评审应包括评价改进的机会和对供应链安全管理体系进行修改的需求,包括安全管理方针和安全目标指标以及威胁与风险的修改需求。应保存管理评审的记录。

为响应来自工业安全管理标准方面的需求,ISO 28000 标准不断发展,最终目的是提高供应链安全。作为高层次的管理标准,能促使组织建立一套全面的供应链安全管理体系。它需要组织对其运作的安全环境进行评估,并确认是否采取了足够的安全措施以及



是否遵守法律法规和其他要求。如果通过这些过程识别出安全需要，组织应实施相应的机制和过程以满足这些需求。ISO 28000 的开发是为满足行业对安全管理体系的需求，最终目标是改善供应链的安全。它是一个能使组织建立全面的供应链安全管理体系的高层次的管理标准，要求组织评估其运作所处的安全环境，以确定其既有的安全措施是否足够，是否已存在组织需遵守的其他法规要求。由于供应链本质上是动态的，一些管理着多条供应链的组织，可能将其服务提供者符合政府或 ISO 供应链安全标准作为进入其供应链的条件，以简化安全管理[ISO 28000]。

2. ISO 28001[ISO 28001]

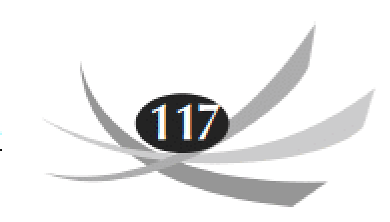
供应链安全管理系统需求有许多来源，ISO 28001 文档用于协助满足 ISO 28000 需求的供应链安全管理系统的认证，它的内容可以用于支持基于其他指定的供应链安全管理系统需求的认证。具体来说：为获取 ISO 28000 的认证机构（或者其他供应链安全管理系统需求集合）的认可提供协调性指导；定义符合 ISO/PAS 28000 需求（或者其他供应链安全管理系统需求的集合）的供应链安全管理系统的审计和认证规则；为客户对他们的供应商获得认证的方式提供必要的信息和信任。组织的供应链安全管理系统的认证是组织确保供应链安全管理符合其政策的方式。ISO 28001 指出了认证机构的需求。满足这些需求可以确保认证机构的供应链安全管理系统认证能以可胜任的、可持续的和可靠的方式运行，从而简化了这类机构的认证以及在国际对认证的认可。它是简化国际贸易利益中的供应链安全管理系统认证的基础[ISO 28001]。

ISO 28001 还用于正在接受认证的组织开发自身的供应链安全管理系统（包括 ISO 28000 供应链安全管理系统、其他指定的供应链安全管理系统需求集、质量系统、环境供应链安全管理系统或者职业保健以及安全供应链安全管理系统），除了指定的相关立法需求，它可用于组织决定如何安排各种组件。各种供应链安全管理系统组件的集成程度根据组织的不同而不同。因此对经过 ISO 认证的认证机构可以考虑涉及更广泛的供应链安全管理系统集成[ISO 28001]。

ISO 28001 的输出内容有：定义供应链边界的覆盖声明；通过记录供应链漏洞来定义安全威胁场景的安全评估，以描述每个潜在安全威胁场景的影响；安全计划，用于描述管理安全评估定义的威胁场景的安全措施；培训项目，设置了安全人员如何被训练来满足他们分配的安全职责。进行安全评估需要产生安全计划如图 5-2，ISO 28001 可以协助组织识别安全威胁（安全威胁场景），分析人们如何将安全威胁场景变成威胁事件，根据观察到的供应链的当前安全状态，确定对于每个安全威胁场景供应链的脆弱性进行专业的判断。如果供应链对某个安全场景的脆弱性是不可接受的，组织将采取额外的程序或者操作变换来降低发生的可能性或者发生后的影响，这些都称为对策。根据系统的优先事项，将对策纳入到安全计划中，从而将威胁降低到可接受的水平[ISO 28001]。

3. ISO 28003

ISO 28003 用于执行供应链管理系统的审计和认证，定义了在进行审计和认证/注册一个客户端组织时，认证机构的最低需求以及相关的审计认证需求。供应链安全管理系统的认证是第三方的合格性评估活动（见 ISO/IEC 17000:2004 的第 5.5 条款）。执行这项活动的团体在 ISO 认证体中称为第三方合格性评估团体。供应链安全管理系统的认



证应该由像国际宇航联合会(International Astronautical Federation,IAF)这样已认证的机构进行实施。这个国际技术规范可以被任何供应链安全管理系统评估中的个体使用[ISO 28003]。

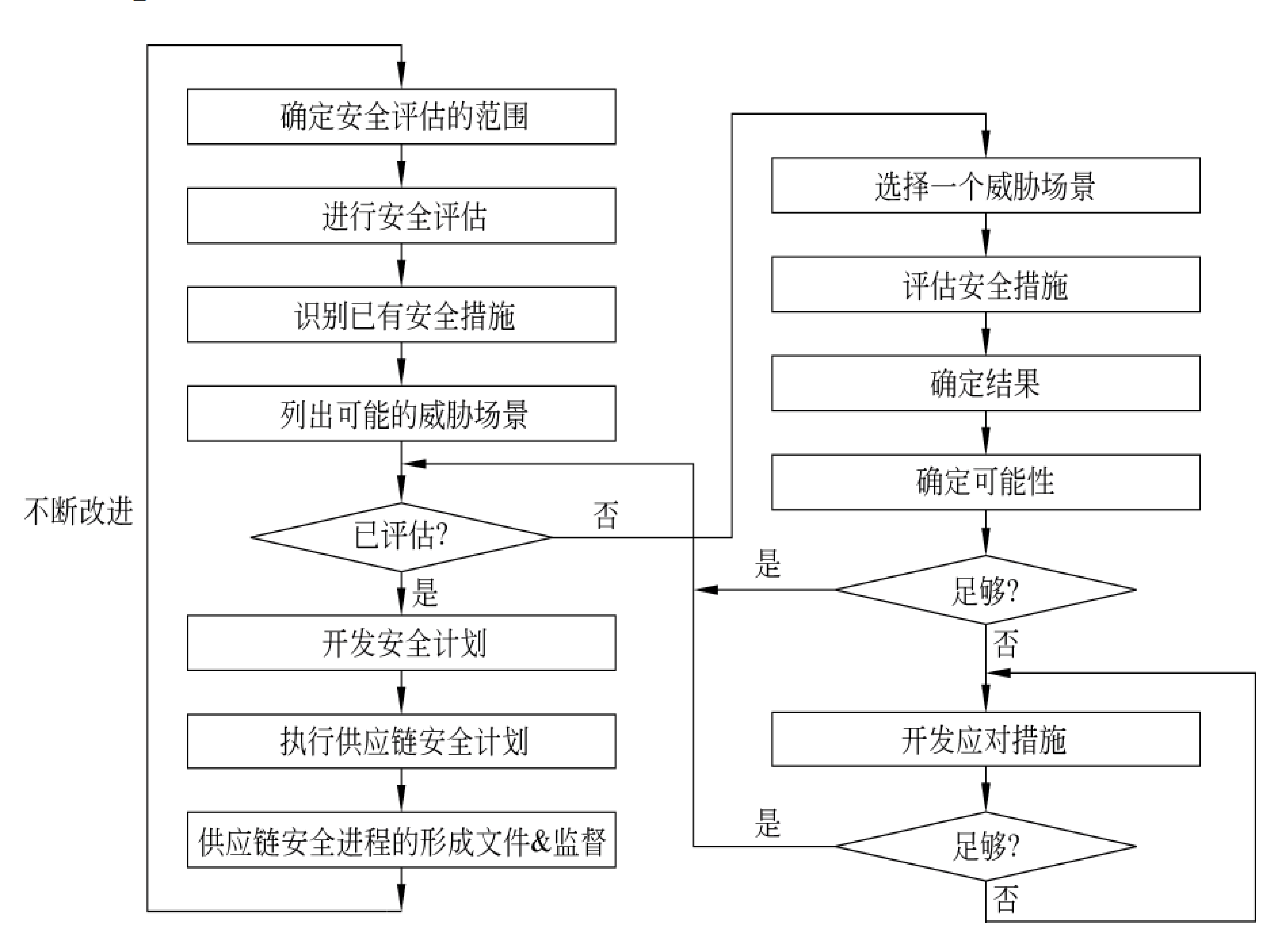


图 5-2　ISO 28001 运行过程[ISO 28001]

4. ISO 28004

ISO 28000与ISO 9001：2000(质量)以及ISO 14001：2004(环境的)管理系统标准是兼容的。它们有助于质量、环境以及供应链管理系统的集成。ISO 28004是为了响应供应链管理系统标准以及标准的实施的需要而开发的。ISO 28004在每个条款/分条款开头,给出来自ISO 28000的完整需求,然后给出相关的指导[ISO 28004]。

5.2.3　ISO 28000的应用

ISO 28000的安全管理体系主要应用于以下两方面。

1. 提供权威认证

DP World(迪拜港口世界公司),世界上主要的全球集装箱港口码头经营者之一,获取了世界上第一张ISO 28000合格证书,其他包括HP、NIKE、IBM等国际公司[LH2010]。

劳氏质量认证公司就供应链安全管理体系正式推出ISO 28000这一供应链安全管理体系认服务。ISO 28000是应运输和物流行业对共同安全管理标准的需求而提出的,其最终目标是改进供应链的全面安全。它能帮助行业各部门审核安全风险并实施控制和减轻风险来管理供应链潜在的安全威胁业务原则如质量安全和客户满意度的管理方式相同。劳氏质量认证公司使用其被认可委员会所认可的程序和过程提供全范围的验证和认证的服务。一旦认可委员会对本标准的认可工作准备就绪,劳氏所颁发的所有证书都将

很快获得认可标记[SY2007]。

国际领先的化工供应链管理服务商上海春宇供应链管理有限公司宣布其正式通过德国莱茵 TUV 的 ISO 28000:2007 供应链安全管理体系认证。这也标志着春宇供应链成为中国化工行业企业中第一家通过该认证的公司。该认证旨在提高供应链的安保管理水平,降低经营风险,提高企业竞争力,保障供应链的可持续发展。在通过 ISO 28000:2007 管理体系之前,上海春宇供应链管理有限公司不断寻求标准化管理,已经分别成功通过 ISO 09001 质量管理体系认证、ISO 14001 环境管理体系认证和 ISO 27001 信息安全管理体系认证[TJHG2011]。

中国质量认证中心(CQC)于 2007 年 9 月着手研讨"ISO/PAS 28000 供应链安全管理体系规范"的应用,是最早进行试点的国内认证机构。2008 年 9 月,ISO 28000 已正式进入国家标准备案程序,争取获取认可资格并将 ISO 28000 在物流行业和其他领域予以推广[LH2010]。

2. 与其他标准兼容,提供系统的管理方法

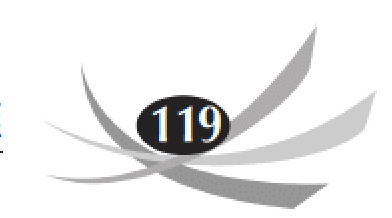
ISO 28000 是唯一真正的全球供应链安全管理系统。与其他系统标准不同的是它的安全管理系统(SMS)的特殊性,ISO 28000 的术语与 ISO 14001 和 ISO 9001 是类似的,可以互相参阅。它和 ISO 14001 使用相同的基于风险的确认安全风险和评估风险的方法。ISO 28001:2005 与 ISO 9001:2008(质量管理体系)及 ISO 14001:2004(环境管理体系)是兼容的,其设计是为了帮助在一个组织内把质量管理体系、环境管理体系和供应链安全管理体系整合起来。该规范是以策划-实施-检查-行动(改进)为基础的管理体系,模仿了公认的 ISO 14001 的标准。这意味着已经熟悉基于风险的方法的组织在分析供应链安全风险和威胁时可以运用相似的方法[LH2010]。

ISO 28000 提供了一套全球供应链安全管理的系统方法,提供了实际的和以商业为中心的风险管理方法作为有效安全管理的关键因素。它确保关键业务决策是基于主动和有效的风险评估进程。实施 ISO 28000 使 YCH 能够衡量它的安全管理系统,通过一种现实的、可持续的和具有成本效益的方式来管理公司在亚太地区网络设施的所有安全需求。ISO 28000 随着时间的推移将成为全球基准,并成为最重要的供应链国际标准。作为供应商选择和投标进程的先决条件,它成为了供应链产业的国际组织的通用语言。

5.2.4 ISO 28000 的意义

无论何种类型组织以及规模,ISO 28000 适用于所有涉及制造、服务、储存及运输的各类组织,关注各类威胁,广泛的应用范围使其成为最为综合性的供应链风险管理体系,致力于建立安全的供应链及促进跨边界货物流通。ISO 28000 把供应商、制造商、分销商、最终客户紧密地联在一起,也使得企业的经营活动更为有效,运作成本更为低廉。配送、物流到供应链,国际物流的发展一直伴随着管理流程的创新和技术手段的创新。进入 21 世纪之后的物流主题,反映了物流产业的一系列变革,而供应链管理创新,成为企业发展的核心竞争力之一。

ISO 28000 还强调在运输工具和货物快速流通的同时提高安全性,并取得了供应链安全认证的组织,可接受规定的优惠待遇。我国物流产业起步晚、发展慢,不同区域、不同



企业发展程度参差不齐。我国物流的主体,停留在传统的运输、仓储、配送阶段,与以美国为主体的国际物流形成了较大的反差。供应链安全管理水平领先的企业,掌握了物流和供应链管理的核心技术,就能够在市场上崭露头角,获得竞争优势。

ISO 28000的优势在于:规章制订者/相关权力机关、顾客/潜在顾客和其他相关组织展示一个有力且安全的供应链管理体系,获取了利益相关方信心;确保一个供应链内服务提供者的方法途径的协调一致性;可以证实组织满足客户要求的能力,以获取客户满意度;通过评估安全风险,实施控制措施和降低风险的途径来管理供应链潜在的安全隐患和影响,较好的实现了风险管理;ISO 28000是一个以策划-实施-检查-改进(PDCA)循环原则为基础的管理体系,以公认的ISO 14001标准为原型,已经熟悉ISO 14001运用的立基于风险的方法的组织在分析供应链安全风险和隐患时可以使用类似的方法,即方便整合;用于向海关当局证明组织管理供应链内部安全问题的能力,当组织考虑申请成为合格的经济运营商(AEO)要满足许多要求时,实施ISO 28000就变得更加重要[WZ3]。

ISO 28000区别于其他标准的是其采用管理系统方法而不是简单的检查清单,关注过程并确保持续改进。目前,ISO 28000经受住了考验并证明了它的成功。ISO 28000标准帮助组织增强供应商的控制,及供应网络的可见性和效率,同时减低成本及增进收益[WZ4]。

5.3 ISO/IEC 27036

ISO 27036是国际标准化组织(ISO)和国际电工委员会(IEC)的联合技术委员(JTC1)信息技术分委员会(SC27)制定的ICT信息安全标准的技术编号,是从供应链的角度出发专门制定的信息安全管理国际标准,在如何保护供应商关系中的信息方面为供应商和采购商提供需求和指导。

ISO/IEC 27036包括多个部分:ISO/IEC 27036-1(2012.2.1-2012.4.1)是信息技术-安全技术-供应商关系信息安全-第一部分:概念及概述;ISO/IEC 27036-2(2012.1.30-2012.4.1)是信息技术-安全技术-供应商关系信息安全-第二部分:通用要求;ISO/IEC 27036-3(2012.1.30-2012.4.1)是信息技术-安全技术-供应商关系信息安全-第三部分:ICT供应链安全指南;ISO/IEC 27036-4(制定中)是信息技术-安全技术-供应商关系信息安全-第四部分:外包安全指南;ISO/IEC 27036-5(制定中)是信息技术-安全技术-供应商关系信息安全-第五部分:云安全服务指南。图5-3提供了有关这个多重标准的抽象结构[ISO 27036-1]。

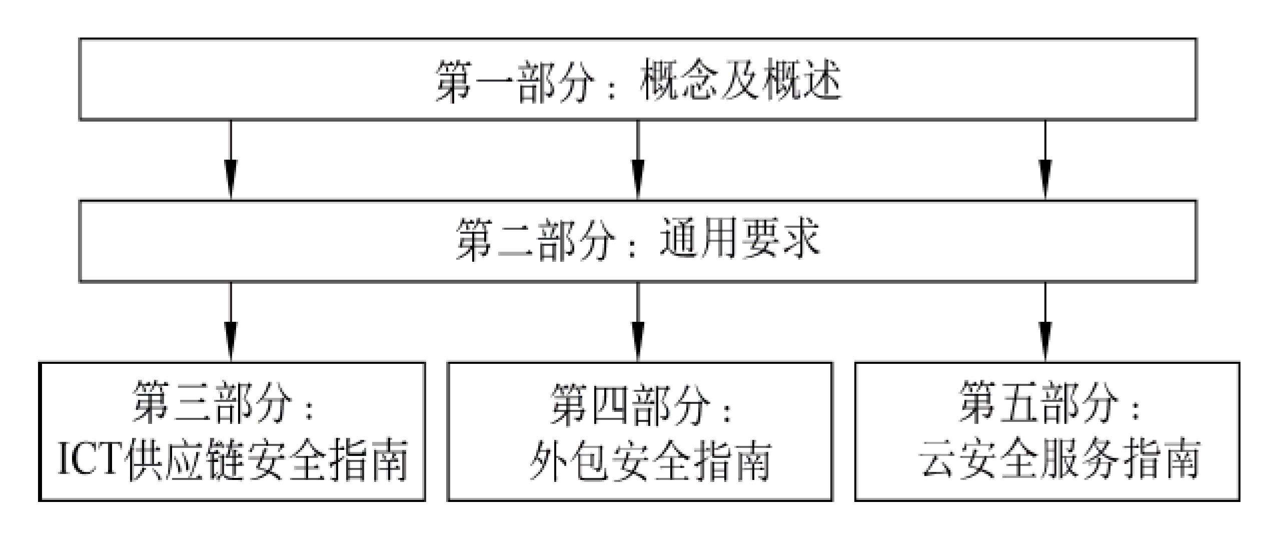


图5-3 ISO/IEC 27036的结构[ISO 27036-1,P9]

5.3.1 ISO/IEC 27036的产生背景

借助遍布全球的供应链，信息和通信技术（ICT）产品和服务在世界范围内不断研发、集成及配送。ICT 产品需要使用诸多供应商提供的组件装配而成。ICT 服务（贯穿整个系统生存周期）也需通过多层外包及供应链才能实现。采购商不可能通过供应链的一环或者两环获悉硬件、软件及服务提供商的作业情况。随着“接触”ICT 产品和服务的机构和人数的激增，想要获悉产品和服务的生成作业情况可谓难上加难。ICT 供应链可视性、透明性及可追溯性的缺失，给采购机构带来了极大的风险[ISO 27036-1]。

信息作为组织的重要资产，需要得到妥善保护。但随着信息技术的高速发展，特别是 Internet 的问世及网上交易的启用，许多信息安全的问题也纷纷出现：系统瘫痪、黑客入侵、病毒感染、网页改写、客户资料的流失及公司内部资料的泄露等等。这些已给组织的经营管理、生存甚至国家安全都带来严重的影响。安全问题所带来的损失远大于交易的账面损失，而缺乏系统的管理思想也是一个重要的问题。所以，需要一个系统的、整体规划的信息安全管理体系，从预防控制的角度出发，保障组织的信息系统与业务之安全与正常运作。在这种形势下，国际标准化组织与国际电工委员会制定了从供应链角度出发的 ICT 信息安全管理的国际管理标准[ISO 27036-1]。

5.3.2 ISO/IEC 27036的内容

ISO/IEC 27036-1(2012)是信息技术-安全技术-供应商关系信息安全-第一部分：概念及概述，它是 ISO/IEC 27036 大部分标准中的介绍性的部分，为相对应的安全组织的信息和基础设施处于多供应商关系环境下的挑战提供了概述。它还介绍了在 ISO/IEC 27036 其他部分所用到的一些概念[ISO 27036-1]。

ISO/IEC 27036-2(2012)是信息技术-安全技术-供应商关系信息安全-第二部分：通用要求，为定义、实施、操作、监控、评审、保持和改进供应商关系管理规定了通用性的信息安全要求。这些要求覆盖了产品和服务的采购、供应的所有情况，例如制造业或装配业、业务过程采购、知识过程采购、建设经营转让和云计算服务，适用于所有类型、规模和性质的组织。通过建立这些要求，无论获取方还是供应商都实施了大量的基础过程来支持整体的活动，这些基础过程包括但不限于：治理、业务管理、运营和人力资源管理以及信息安全[ISO 27036-2]。

ISO/IEC 27036-3(2012)是信息技术-安全技术-供应商关系信息安全-第三部分：ICT 供应链安全指南。虽然最初的出发点不是为了管理和控制 ICT 供应链的安全风险，但在美国标准化专家的努力下，目前 ISO/IEC 27036 已经为 ICT 供应链安全制定了子标准，即 ISO/IEC 27036-3《信息和通信技术供应链风险管理》。提供了 IT 软件、硬件和服务的供应链安全指南，将信息安全过程和实践整合到系统和软件的生命周期过程中，专门考虑了与组织及其技术方面相关的供应链安全风险（例如插入恶意代码或仿冒 IT 产品）。ISO/IEC 27036-3 是第一部针对 ICT 供应链安全提出的国际标准，意义重大[ISO 27036-3]。

ISO/IEC 27036-4(制定中)是信息技术-安全技术-供应商关系信息安全-第四部分：

外包指南。组织外包各种服务，信息安全会依照服务类型和情况有很大不同。例如，当信息外包处理时，供应商可能会访问采购商的信息，因此会给信息安全带来更大的风险。根据外包所需的采购商和供应商的系统互联性，供应商可能会遇到类似于 ITC 服务信息安全风险的额外信息安全风险。第四部分为采购商和供应商如何应对与外包相关的信息安全风险提供了准则。它建立在第二部分要求的基础之上，并提供了可以提高第二部分高级要求的额外方法。

ISO/IEC 27036-5(制定中)是信息技术-安全技术-供应商关系信息安全-第五部分：云安全服务指南。

后来第 4 部分被删除，将原来的第 5 部分改成第 4 部分。

5.3.3 ISO/IEC 27036 的应用

ISO/IEC 27036：信息技术-安全技术-供应商关系的信息安全包括收购者和供应商之间关系的信息安全，为各方提供恰当的信息安全管理。它适用于所有组织(例如，商业化企业，公共部门机构，非盈利机构和合作伙伴)，指定了信息安全需求并给出供应商关系指南(例如，识别和分类供应商；同意、监控和改变供应商；退出)。它涵盖了所有类型的供应商关系，包括外包、产品和服务采购，云计算，ICT 和其他类型的有信息安全问题的供应商关系(例如，电力、人力资源、设施管理)。

ISO 27036 标准主要用于 ICT 供应链中购买或提供 ICT 产品和服务的各类机构，主要侧重于第一采购商和第一供应商所构建的初始链，但也适用于整个供应链，包括从第一供应商实现角色转换而变成采购商等一系列环节。该标准旨在转换角色或每次在供应链中出现新的采购商-供应商链后，依然可使用同样的准则。执行此国际标准，可实现信息的安全传输，从而实现整个供应链信息安全风险的可视性和透明性。ISO 27036 涉及供应商关系的信息安全，涵盖许多不同的情景。想要提高在 ICT 供应链中的可信度，各机构应首先定义自己的信任底线，评估供应链活动中的风险，明确并实施适宜的风险识别和缓解方法，降低 ICT 供应链中的不安全因素的风险。

ISO 27036 标准主要在三方面提供指导：对由 ICT 供应链的地理位置分散而引起的安全风险获得可见性并进行管理；将信息安全程序和实践集成至系统和软件的整个生存周期；针对由 ICT 产品和服务的全球供应链引起的风险，建立响应，包括能够影响到使用此产品和服务的机构安全的所有风险。具体来说主要通过系统生命周期流程、信息安全管理系统 PDCA 流程和风险管理实现。

1. 采用系统生存周期流程[ISO 27036-3]

ISO/IEC 15288 和 ISO/IEC 12207 分别包含了系统的生存周期流程和软件的生存周期流程。两个标准都提供了一系列适用于特定系统或软件环境的相同流程。ISO/IEC 12207 是 ISO/IEC 15288 应用的特定实例。两个标准都可用于任何生存周期或生存周期模型，并且列举了可用于任何生存周期或生存周期中任何阶段的一系列流程。例如，配置管理流程即可用于系统或软件的开发阶段，又可用于生存周期的运行和维护阶段。

ISO/IEC 15288 的生存周期流程可用于任何人为构建的系统。ISO/IEC 12207 详细说明了软件密集型系统流程，并添加了一些软件特定流程。这两个标准的用户可以选择

使用两个标准中的流程。目的和结果声明对每个流程进行了总结性描述。另外，活动分解对每个流程进行了细节阐述，其中每项活动都是一个任务集。

生存周期流程有利于采购商和供应商就信息安全问题制定预期的严格性和可核查性等级。采购商可在内部实施生存周期流程，用于更加严格地建立和管理供应商关系。供应商可实施生存周期流程，帮助论证供应商就供应商关系问题应用于系统和软件流程的严格性。鉴于这些流程的制定有助于采购商和供应商双方着手解决 ICT 供应链的风险问题，故应将更多的 ICT 供应链风险管理活动整合到这些流程之中。标准中第 5.5 条提供了 ICT 供应链的风险管理方法的概括说明。第 6 条提供了这些 ICT 供应链的风险管理特定活动在每个生存周期流程的映射。采购商应根据第 5.2 条介绍的供应商的风险等级，选择关于其组织的供应商关系能力以及个人供应商关系的活动。

2. 针对生存周期流程使用了信息安全管理系统 PDCA 流程[ISO 27036-3]

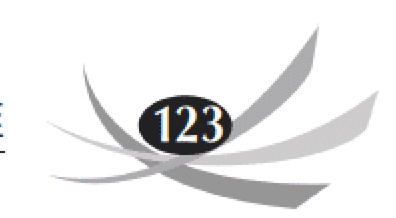
PDCA 循环又叫戴明环，是美国质量管理专家戴明博士提出的，它是全面质量管理所应遵循的科学程序。全面质量管理活动的全部过程，就是质量计划的制订和组织实现的过程，这个过程就是按照 PDCA 循环，不停顿地周而复始地运转的(这里，P 为 Plan(计划)，D 为 DO(执行)，C 为 Check(检查)，A 为 Action(处理))。

ISO/IEC 27001 提供了基于风险的流程，用于在定义范围内使用信息安全管理系统(ISMS)。采购商和供应商组织使用信息安全管理系统，有助于双方着手解决 ICT 供应链风险，并满足解决风险所需的特定信息安全控制和流程的需要。此处假设信息安全管理系统的范围包括组织中建立和维护采购商和供应商关系的特定部分。如果组织将某些风险定义为 ICT 供应链中固有的，则应选择特定控制方法降低此类风险，为确保组织完全解决此类风险，还可能增加扩展控制。第 5.5 条解决了安全控制的使用。第 6 条探讨了适用于单个生存周期流程中的特定安全控制。ISO 27036 规定供应商可通过阐明其同 ISO/IEC 27001 标准的一致性向采购商证明自身具有的严格性等级。

3. 生存周期流程中的 ICT 供应链风险管理[ISO 27036-3]

(1) 协议流程。组织是 ICT 产品和服务的生产商和用户的统称。产品和服务的生产商和用户间的关系通过签订协议而建立。在系统中，组织可同时或相继扮演采购商和供应商的角色。当采购商和供应商同属于相同组织的情况下，仍然推荐使用协议流程，但协议可以是非正式协议。协议流程包括采购流程和供货流程。本标准为采购流程提供了详细的指导并指出了供货流程应当包含的活动。

(2) 组织项目使能流程。组织项目使能流程用于确保所需资源能够使项目满足组织的利益相关方的需要和期望。组织项目使能流程建立了项目执行的环境。除非特定声明，否则这些流程既适用于采购商，又适用于供应商。生存周期模型管理流程用于定义、维护及确保政策、生存周期流程、生存周期模型及组织使用规程的可用性。在此流程中应考虑 ICT 供应链风险管理，但是无需根据 ICT 供应链风险管理而采取额外的特定操作。为了解决 ICT 供应链风险管理相关的风险，标准还指出了供应商组织的基础设施管理流程需包含的活动。项目组合管理程序的目的在于启动并支持必要的、足够的及适合的项目，以满足组织的战略目标。在此流程中应考虑 ICT 供应链风险管理，但是无需根据 ICT 供应链风险管理而采取额外的特定措施。组织应针对特定 ICT 供应链问题以及如



何解决这些问题对员工进行培训，即执行人力资源管理流程。为了解决ICT供应链风险管理相关风险，采购商和供应商还需进行质量管理流程，在产品的生存周期中，将弱点与脆弱性测试整合至质量管理活动中。

(3) 项目流程。项目流程涉及系统和软件工程项目的严格的项目管理和项目支持，包括跨越供应链或多重供应链的项目管理和项目支持。除非特别声明，否则此类流程既适用于采购商，又适用于供应商。由于项目中涉及的ICT产品和服务的生产和交付，跨越地理位置分散的并受多重实体的控制供应链，项目规划及项目计划整合时，需要考虑需求对进度的影响等。项目评估和控制流程的目的在于确定项目状态与直接项目计划执行，以确保项目执行符合计划和进程表，不超出计划预算并满足技术目标。在此流程中应考虑ICT供应链风险管理，但是无需根据ICT供应链风险管理而采取额外的特定操作。决策管理流程的目的在于，当存在多种供选方案时，选择最为有利的项目操作方法。在此流程中应考虑ICT供应链风险管理，但是无需根据ICT供应链风险管理而采取额外的特定操作。配置管理对于了解产品、系统、产品和系统元素、相关文档和供应链本身的更改(包括更改者)至关重要。为确保ICT供应链问题得以妥善解决，标准规定采购商和供应商的配置管理流程中应包含的下内容，以解决特定ICT供应链风险管理相关的风险。此外，标准还对信息管理流程和和测量流程做了指导。测量流程的目的在于搜集、分析和报告机构内相关产品开发和操作执行的数据，用于支持流程的有效管理并客观说明产品质量。测量流程中没有ICT供应链风险管理的具体方面。ISO/IEC 27004就信息安全测量提供了指导，可用于制定和实施特定的措施，以解决ICT供应链风险管理问题。

(4) 技术流程。技术流程定义了相关需求，将需求转化为产品和服务，并解决产品和服务废弃前的使用问题和可持续问题。除非特定声明，否则这些流程既适用于采购商，又适用于供应商。利益相关方需求定义流程的目的在于定义系统需求，使系统在指定的环境下，为用户和其他利益相关方提供所需要的服务。需求分析流程的目的在于将利益相关方对所需服务需求驱动的观点转换为能实现所需服务的产品的技术观点。结构设计流程的目的在于，集成满足系统要求的解决方案。执行流程的目的在于实现一个特定的系统元素。集成流程的目的在于根据结构设计组装一个系统。验证流程的目的在于确定系统满足特定的设计要求。转移流程的目的在于建立一种在操作环境下提供利益相关方需求中指定服务的能力。确认流程的目的在于提供客观证据，证明系统服务在使用时符合利益相关方的要求，在其使用环境中达到预定使用目的。为了解决ICT供应链风险管理相关的风险，标准还对运行流程、维护流程和废弃流程进行了指导。维护流程的目的在于保持系统提供特定服务的能力。废弃流程的目的在于结束系统中实体的使用。废弃可在系统或元素生存周期中的任何一个点发生，包括电子和非电子媒介的废弃。

5.3.4 ISO/IEC 27036的意义

全世界大多数组织，无论其规模大小或活动领域是什么，都可能与提供某种产品和服务的各类供应商有联系。这些供应商可以对买方的信息及信息系统进行直接的物理和/或逻辑访问，或者为其提供信息处理中所涉及的元件(软件、硬件、活动进程或人力资源)。ISO 27036国际标准在供应商关系中实施了信息安全管理和控制并对其进行了对应的风

险评估和处理,为 ICT 产品和服务、清洁服务,咨询服务,外包应用(ASPs),以及云供应商(SaaS、PaaS、IaaS)关系提供了指导。它从供方和买方两个角度描述了信息安全问题,要求供方和买方实施或计划实施一系列基本流程(例如,管理、企业管理、运营及人力资源管理)来支持企业目标的完成及供方/买方关系中双方目标的实现。

ICT 供应链在世界范围内的发展和壮大使得采购商不可能通过供应链的一环或者两环获悉硬件、软件及服务提供商的作业情况,造成 ICT 供应链可视性、透明性及可追溯性的缺失。ISO 27036 的实施尤其增加了 ICT 供应链的可视性和可追溯性,增进了采购商对产品产地及研发或集成产品作业情况的了解,如果发现问题产品,可获取问题材料及涉及人员的可靠证据。

5.4 ISO/IEC 15026

ISO 15026 是国际标准化组织(ISO)和国际电工委员会(IEC)的联合技术委员(JTC1)信息技术分委员会(SC27)联合起草制定的系统与软件确保国际标准的技术编号,用以应对软件和系统的缺口风险。这个标准包括四部分:15026-1(2008):概念和词汇:最初的技术报告;15026-2(2008):确保案例:包括对确保案例内容、确保案例生命周期以及作为确保案例本身信息条款的需求;15026-3(2011):系统完整性级别(1998 年标准的修订):将确保案例的完整性级别与有确保案例和没有确保案例时的需求联系起来;15026-4:生命周期中的确保:陈述产品和包括项目计划在内的确保案例的并发开发和维护。

5.4.1 ISO/IEC 15026 的产生背景

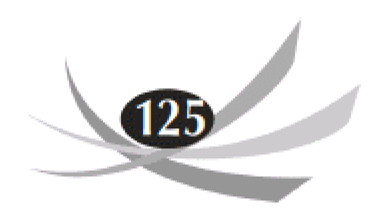
确保问题空间:大规模的系统代表复杂的供应链整合;这些系统来自多个供应商,这些供应商雇佣世界各地的人们;大多数系统依靠软件实现它们的大部分功能;建立可信的安全软件的技术是不够的:一是开发软件的能力跟不上硬件进步的步伐;二是不能构建可以预期的复杂的软件密集型系统。在软件和系统确保以及其他密切相关的领域,许多专业和附属专业使用不同的词汇来表示相同的概念。例如保障、安全、可靠、隐私等领域的确保都使用一些独特的概念和词汇表示一些常见的概念,这将导致跨学科工作时由于隔离造成的不明智的交易决定。为了应对软件和系统的缺口风险,国际标准化组织(ISO)与国际电工委员会(IEC)成立的联合技术委员会(ISO/IEC JTC)出版了 15026 国际标准,旨在提供一个可以使不同的学科可以联系到一起的总体框架,与现有的生命周期进程标准相联系[ISO 15026-1]。

5.4.2 ISO/IEC 15026 的内容

ISO 15026 国际标准主要提供了一系列的术语、确保案例和生命周期进程进行联系。ISO 15026 标准一共分为如下 4 部分。

1. ISO 15026-1 概念和词汇(最初的技术报告)[ISO 15026-1]

这个技术报告建立了对国际标准的核心概念和准则的共同理解的基础,它有关 ISO/



IEC 15026 国际标准的整个部分，标识了在 ISO 15026 中使用的或者不使用的现有词汇定义并定义了额外需要的词汇，包括问题、概念和术语使用中的条款。在软件和系统确保及其相关领域，许多专业和附属专业共用概念，但是这些概念使用不同的词汇表示不同的观点。这个技术报告提供了统一的底层概念集合，使可理解的观点的创建以及跨领域的术语的使用成为现实。因此，它为细化、讨论和记录协议、有关概念的基本原理、跨越 ISO 15026 各部分使用统一词汇提供了基础。ISO 15026-1 强调了理解软件和系统确保领域需要的概念，尤其是对 ISO 15026 国际标准第 2～4 部分进行了概念上的准备。另外，它促进了共享概念和问题基础上的领域内知识掌握，强调了属性、应用程序以及技术范围内概念和术语的使用。

2. ISO 15026-2 确保案例[ISO 15026-2]

包括确保案例内容下的需求和确保案例生命周期本身以及计划确保案例的告知性条款。还提供了有关为了覆盖而选择的产品属性的保证声明要求，这些属性通常是因为产品实现中需要信任(产品意味着一个如系统、软件、设备或者服务的过程的结果)。确保案例包括：(1)声明；(2)支持声明的论点；(3)论据以及如何支持论点。确保案例提供了决定不确定性和管理相关风险的焦点，因此成为风险评估和风险管理以及生命周期活动中的计划、设计、获取、展示、维持、监控利益性能的关键因素。它提供了一个通用的术语、概念和结合现有实践中的不同例子的需求的框架。

确保案例是产品必须符合和用于显示足够低的不确定性的处理机制的元素。确保案例的论证是确保案例的主体。一个确保案例使用与多个级别声明和附属声明连同相关的论据和假设相联系的结构化论点来评估高级别声明的完成程度。它还评估成果是否符合需要的不确定性。高级别声明、相关不确定性以及后果的论证是合理的风险管理和获取适当可信性的基础。

原则上，确保案例支持的声明可用于产品(例如，系统或服务)或者环境的任何属性。这些可能包括(但是不限于)与可靠性相关的属性，例如可靠性、可用性、完整性、可维护性、正确性、精确性、安全性、保密性、可说明性或者可用性；与时间和资源相关的属性，例如处理速度、可调度性、吞吐量以及存储容量；低级别属性例如功能存在性或者更多全局属性例如任务完成。15026 国际标准主要是为了在重要的或者高风险的属性的应用。不同的利益相关者可以以不同的方式使用确保案例来实现各自的目标。

3. ISO 15026-3 系统完整性级别[ISO 15026-3]

ISO 15026-3(替代了 ISO 15026-1998 信息技术系统和软件完整性级别)将确保案例和完整性水平相联系，包括使用和不使用确保案例时的相关要求。它指定了对应完整性水平需求的完整性级别的概念，覆盖了系统、软件、产品以及元素等。主要被以下角色使用：像工业和专业组织、标准组织和政府机构这样的完整性水平的定义者；像系统或软件的开发商和维护商、供应商和集成商、用户和评估者这样为了系统的管理和技术支持的完整性水平的用户。

ISO 15026-3 指定了完整性级别的概念及相应的完整性级别需求。它阐述了定义和使用完整性级别的需求和建议，包括如何将完整性级别嵌入到系统、软件产品、它们的元素以及相关的外部依赖中。ISO 15026-3 应用于系统和软件，用于以下方面：定义完整性

水平，例如行业和专业组织、标准组织和政府机构；为完整性级别的用户提供进行行政和技术上的支持，例如系统或软件的开发者和维护者、供应商和采购商、用户、评估者；帮助供应商和采购商保护交付系统的安全、经济或安全特性。它可以单独或者和 ISO/IEC 15026 的其他部分一起使用，用于各种技术的和专业的风险分析和开发方法。

4. ISO 15026-4 生命周期确保［ISO 15026-4］

ISO 15026-4 阐述了产品的并发开发和维护以及确保计划案例，为执行已经选定的进程、活动和任务提供指导和建议，这些选定的内容用于需要确保声明来选定特别关注属性的系统和软件。ISO 15026-4 指定了进程、活动和任务的独立属性名单以获取声明和展示声明成果。ISO 15026-4 在已定义的生命周期模型和系统和/或软件生命周期管理进程集合中建立了进程、活动、任务、指导和建议。

为了使供应商对他们的产品做出符合系统、产品或服务的安全性、保障性和可靠性的确保论证，ISO 15026 将确保案例作为启动机制。一个确保案例至少要包括一个合理的、结构化的可审计的论点，以及令人信服的、可理解的、有效并有界的论据来证明论点，系统的产品足以在整个生命周期中发挥作用。由此可得出各部分标准的内在联系，如图 5-4 所示。

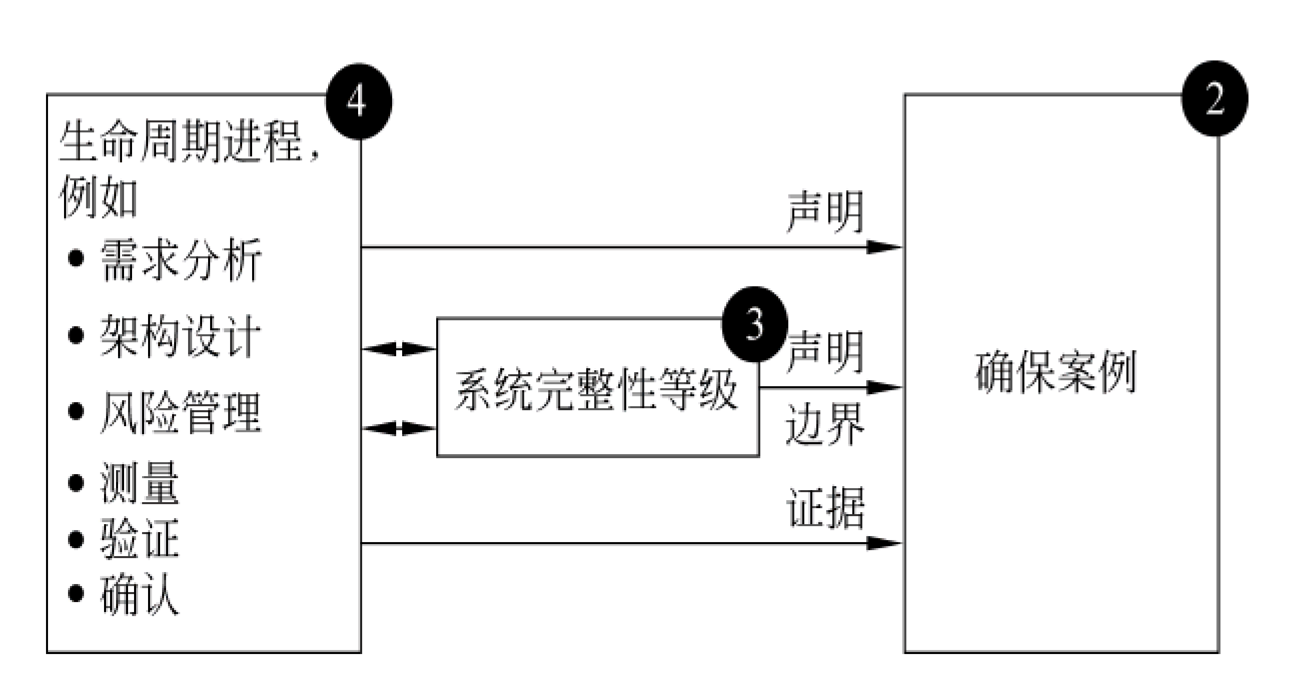


图 5-4 各部分标准的内在联系［RH］

5.4.3 ISO/IEC 15026 的应用

ISO 15026 提供了包括系统和软件产品的开发、运作、维护和处理在内的生命周期的需求，这些需求对于安全、保障、可靠等属性非常重要。确保案例是计划、监控、获得和展示成果、属性维持以及相关决定支持的中央产品。生命周期进程的确保案例的需求间的相互作用对 ISO/IEC 15288、ISO/IEC 12207 的进程做了规范的解释，除了 ISO/IEC 15289，都给出了由这些进程得出的信息产品的需求。ISO 15026 目的是协助那些希望将 ISO/IEC 15288 和 ISO/IEC 12207 的条款应用于需要拥有关键属性的系统用户［RH］。

图 5-5 描述了和生命周期进程相关的几个标准的关系。图的底部是很多标准的基础，提供了通用词汇、进程结构以及描述这些进程的公约。其他描述的标准建立在这个基础之上，ISO/IEC 15288 和 ISO/IEC 12207 分别为系统和软件提供了生命周期进程。它们是彼此协作的，因此有助于系统的多样化内容。这两个生命周期进程由四个标准支撑，在共有问题上提供了额外的需求和指南：ISO/IEC 15289 是生命周期进程的执行文档；ISO/IEC 16326 是项目管理进程；ISO/IEC 15939 是测量进程；ISO/IEC 16085 是风险管

理进程。此外还有提供额外需求和选定的进程指导的其他标准。ISO/IEC 24748 描述了生命周期进程是如何管理系统或软件的整个生命周期的。ISO/IEC 15026 与其他这些标准是兼容的。

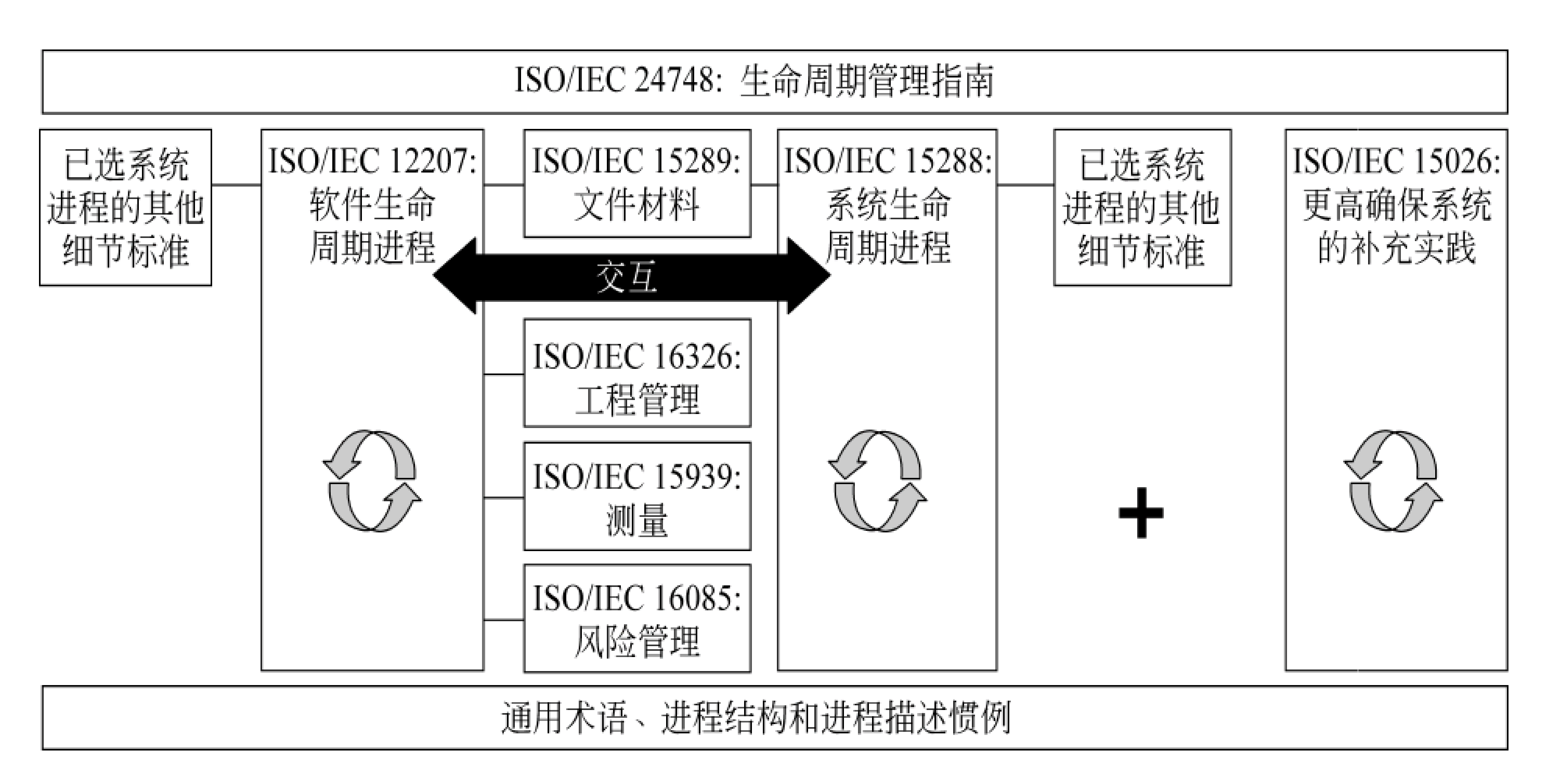


图 5-5 ISO 15026 与其他标准的联系[RH]

ISO/IEC 15288 和 ISO/IEC 12207 中的技术和管理进程,被用于和 ISO 15026 相结合,用于利益相关组织计划用于建立和维护确保案例(确保安全性、保障性、可靠性信息,建立确保论点以及支持它的论据)的确保活动(建立和维护确保计划)。和这个标准相结合的生命周期和测量进程,用于确保活动和产品(监控操作和报告事件;建立独立的安全和保障报告;监督和控制与确保需求相关的活动和产品;陈述确保问题)的管理。计划和实际的确保案例被用于生命周期进程,监督和提高确保活动和产品。ISO 15026 的规定大体上与和产品质量相关的 ISO/IEC 25000 标准系列是一致的,并致力于和信息安全管理系统相关的 ISO/IEC 27000 标准系列、IEC 61508 的许多关于功能安全的部分以及关于可靠性的 IEC TC 56 的许多标准保持一致。然而,除了特别强调,ISO 15026 在对其他标准的使用上不具备依赖性[RH]。

确保案例与选定的生命周期进程的关系以及相互作用,如图 5-6:项目计划进程提供了创建包括确保计划在内的项目计划的焦点。项目评估和控制进程是评估确保需求和采取相应行动的成果的焦点。需求分析进程指出要以可评估的方式指定确保需求。风险管理和测量进程使利益相关组织能够识别和优先考虑相关的安全和保障风险;确定、实施和监控风险和风险缓解计划;执行必要的测量活动并监控相关操作和报告事件。风险管理和考虑到确保的生命周期进程间的相互作用有助于明确风险概况和信息、风险操作请求和信息的管理。测量和考虑到确保的生命周期进程间的相互作用有助于信息需求和信息产品的描述以及支持确保需求的测量反馈[ISO 15026:2007]。

5.4.4 ISO/IEC 15026 的意义

ISO 15026 国际标准提供了一个统一的底层概念集合,使得跨越这些不同领域的观点被理解,术语被明确使用。它提供了一系列的术语、确保案例和生命周期进程进行联系,建立了对国际标准的核心概念和准则的共同理解的基础,为阐述、讨论、记录协议和有

关概念的基本原理、使用统一的词汇以及提供背景信息和讨论基本原理及问题提供了基础。它强调要理解软件和系统确保领域的概念，特别是在 ISO 15026 国际标准的第 2～第 4 部分使用的那些概念。在共享概念的基础上它支持评估在这个领域的知识掌握水平，强调跨越一定范围的性能、应用领域和技术的概念和术语的使用[ISO 15026-1]。

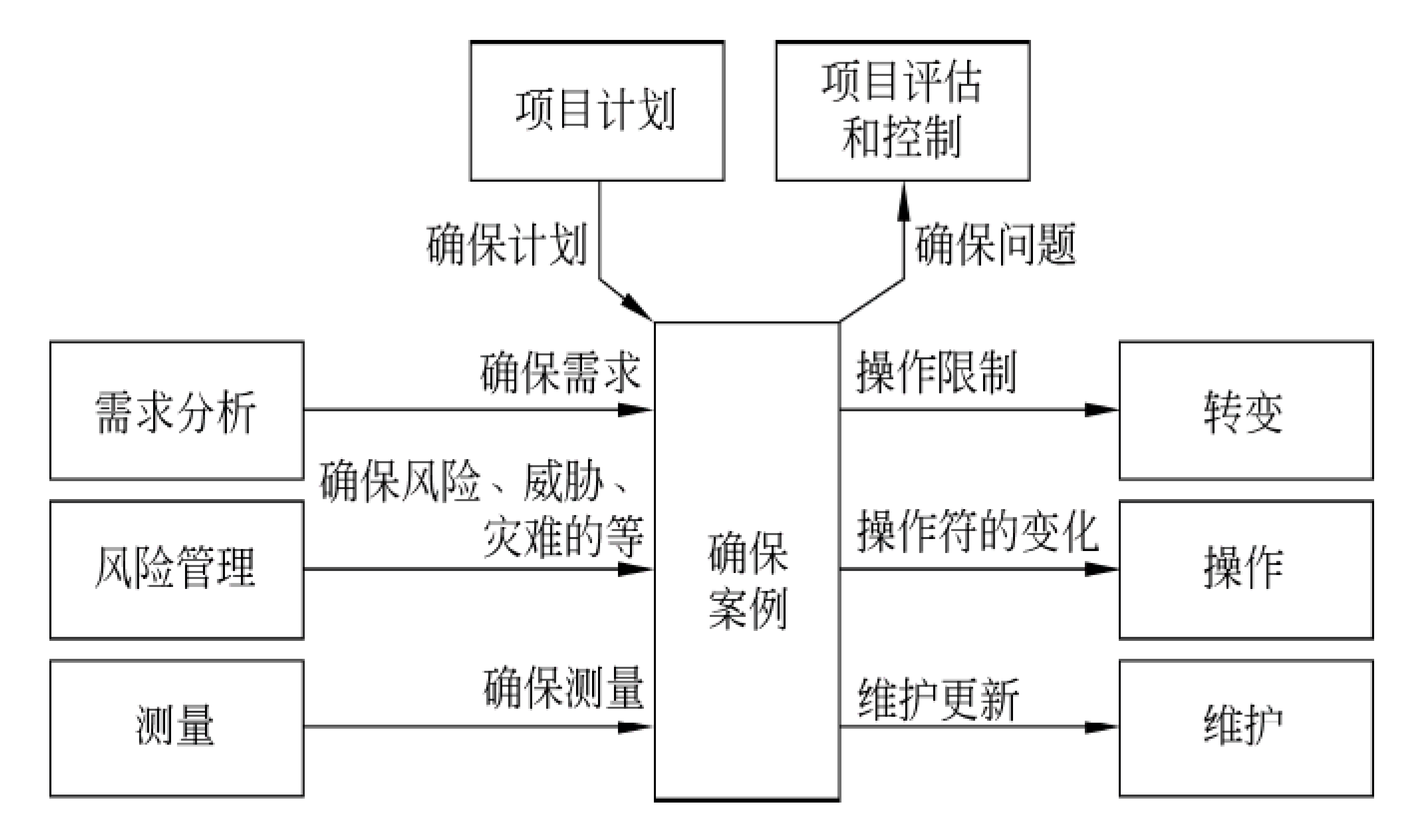


图 5-6 确保案例与生命周期间的相互作用[ISO 15026:2007]

5.5 NISTIR 7622

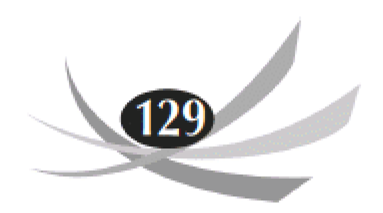
NISTIR① 7622 是美国国家标准与技术研究院(NIST)草拟的网络供应链风险管理指南，旨在购买、开发和运营过程中消除高影响联合信息系统面临的生命周期供应链风险。目前 NISTIR 7622 已出版了两个版本，第一版本于 2010 年 6 月出版，第二版本于 2012 年 3 月出版，在第一版的基础上进一步阐释了供应链风险管理在 ICT 领域的应用，本书以下内容将以第二版内容为准。

5.5.1 NISTIR 7622 的产生背景

信息系统正成为政府机构和正常运转的命脉。然而，随着技术的日趋成熟和全球化的进一步扩展，信息系统及其相关配套设施遭遇安全威胁的几率正在成倍的增加。由于许多供应商都是跨国公司，外包和分包也正在成为一种不可逆转的趋势，使得确保供应链安全成为一项几乎不可能完成的工作。因为急剧扩张的外包趋势在很大程度上降低了供应链的透明性和可追溯性。甚至在美国本土开发的信息系统或组件，也会因在项目过程中采用折中方法，而有意无意间形成漏洞，造成系统结构脆弱，由此引发或加大供应链的风险[NIST 7622-2]。

供应链攻击包括控制系统生命周期中的任一节点，无论是计算机系统硬件、软件还是服务。供应链攻击通常由个人或组织通过商业节点发起，其行为包括窃取核心数据和技

① IR 代表机构间报告，NISTIR 与白皮书类似，可以是一个报告或者会议记录，概述了良好的策略但并不强制实施。这份指南作为 NISTIR 出版是为了检测这些方法对人们的实践是否有指导意义。所有的联邦机构必须实施 SP 中的指南，所以 NISTSP 更具有强制导向性。SP 只要求联邦机构遵循，私人企业除外。所以尽管这是一个供应链文件，主要是为了联邦机构提供建议的，不强制私人机构做任何事。



术、造成系统或架构瘫痪及核心功能无法运行等。对依赖外来实体满足关键政府职能需要产生担心，并且面临他们无法控制也缺少适当评估工具的复杂供应商供应链风险环境，美国政府部门采取了各种方法来应对供应链风险。尽管这些应对措施都以基于安全的考虑事项为基础并且通常采用风险应对原则，但由于此类原则的运营方式不同，这些方法可能会对贸易和创新产生不同程度的影响[NIST 7622-2]。

举例来说，“国家网络安全全面倡议”(2008) 的第11项计划为美国提供了总体策略框架，它指出：在产品、系统和服务的整个生命周期内，必须以战略性的综合方式应对源自国内和全球供应链的风险。应对此风险需要充分了解威胁、漏洞以及与购买决策相关的后果；开发并利用工具和资源，从技术和运营方面降低产品生命周期(从设计到报废)内的风险；制定反映全球复杂市场变化的新购买政策并获取实践经验；与企业合作开发和采纳供应链和风险应对标准及最佳做法[NIST 7622-2]。

在这样的形式下，美国国家标准与技术研究院 (NIST) 草拟了一套做法，旨在购买、开发和运营过程中消除高影响联合信息系统面临的生命周期供应链风险。NIST 草拟的机构间报告(IR)7622(草稿 NISTIR 7622)的认为，重要信息系统及其组件“面临攻击者带来的越来越大的供应链攻击风险，这是因为技术更加复杂，而信息系统基础设施、供应商和攻击者的快速全球化加大了这种风险”[NIST 7622-2]。

5.5.2 NISTIR 7622的内容

NISTIR 7622 第二版阐释了供应链风险管理在 ICT 领域的应用，提供了一套实例，可直接应用于那些级别达到 FIPS(Federal Information Processing Standards，联邦信息处理标准)标准的采购与合同。这些实例对那些当今必须应对来自全球供应商以及有潜在威胁的企业和机构来说，可帮助他们合理规划和管理信息采购、系统开发、系统或系统间运营中遇到的各种问题，并在控制成本、严格执行计划及满足开发需求方面有所改进。在系统开发生命周期过程中使用这些实例时，企业和机构可以有效规避风险。它的读者群应包括信息系统采购方、采购团队、信息系统安全负责人和负责信息系统交付的相关工程师，涵盖为政府和商业机构提供产品、服务和信息安全服务的所有环节[NIST 7622-2]。

NISTIR 7622 指南明确规定了供应链风险管理的参与者，有主管官员、首席信息官、项目总监、项目总监技术助理、法律顾问、测试组、需求分析、系统运营官、首席系统安全官、信息系统安全官、信息技术投资委员，并对其相应职责做了说明。供应链风险管理能力的建立，需要机构成立专用的联合小组，运用技术和相关程序评估、罗列供应链风险；同时，还应制订供应链风险管理政策，设定组织结构、岗位和职责来实施控制。系统运营方应与供应链风险管理小组合作，确保系统、组件和与供应链相关的服务的正常部署与运营。系统运营方、信息系统安全人员以及内部相关人员应该充分了解供应链风险的内涵及其重要性。有可能的情况下，应该由外部第三方专家提供公正的意见和建议[NIST 7622-2]。

NISTIR 7622 并不提供具体的合同语言、威胁评估、完整的供应链安全保障方法或技术来降低供应链风险。取而代之的是一套可执行实例，同时在指南中分别对其进行了简单描述。它的初衷是组织机构和企业能试用它们，并在其可行性、实用性、经济性、存在问

题和优点等各个方面给我们以回馈。因为我们现在所做的只是未来管理供应链风险庞大计划中的第一步。NIST 希望在多次实践后，相关组织结构和方法论能够得到有效试用，然后开发出一套涵盖多领域的供应链风险管理方法，以此作为 CNCI 国家网络安全综合计划的有效体现[NIST 7622-2]。

NISTIR 7622 的重点在于协助大家罗列和控制整个产品生命周期中的所有供应链风险，而非仅仅被动接受产品和系统，在交付后才想办法去控制风险。要知道，个人的努力只能很有限地降低供应链风险，因为在整个供应链中有太多可以影响安全的因素和组成部分。据此，指南围绕整个产品生命周期，运用了一系列组合实例，以最大程度地降低供应链风险。企业和相关机构应根据自身需求、计划和财务状况，选择适合自己应用和采购的实例作为参考[NIST 7622-2]。

作为信息系统服务和组成部分供应商的公司，也就是相关业务和产品的总包商。因此，总包商也应参考本文中提到的一些注意事项。在使用一些专利数据时，总包商们有必要在合同中使用特定语言规定这些数据的使用方式、保存周期、使用人群和适用于哪方面的信息保护法规。在进行发标邀请（RFI）、报价请求（RFQ）、需求说明书（RFP）、合作研究开发协议（CRADA）、产权交付和相关文件的准备中，都应考虑供应链问题。在制订所有协议和采购合同时，务必注意语言的简洁，在需求上做到可衡量和可执行。最大限度地使用现有标准和指南，以增加过程的可信息系统的采购方必须在与供应链相关实施和工作中起主导作用[NIST 7622-2]。

供应链风险评估是通过衡量以及系统被攻破的情况下，可能造成伤害的级别，以及这些级别会对个人、资产，其他机构和国家造成的影响。因此，在实际应用中，机构有必要考虑适用的标准级别，并非所有信息系统都应采纳供应链风险降低方案，比如 FIPS 199 影响标准应该只适用于相关级别的机构。

NISTIR 7622 还强调了保持关注的重要性。一旦系统进入启动阶段，供应商、项目元素、交付和商业流程以及其他因素都可能发生改变。这些改变也许会增加供应链风险。因此，在动作过程中，始终要进行供应链风险管理。务必理解供应链风险，并能及时提供元素修改信息、运作环境、潜在风险和补丁的供应商合作，这样才可有效进行供应链风险管理。在进行组件替换、定制和升级一类技术行为，尤其是不经过考核供应链风险的传统采购流程时应尤其注意其中潜在的供应链风险。废弃子系统同样是一个风险产生的诱因，因为它们已经使用了很长时间，实际上，作为系统组成部分的子系统、组件和技术在废弃时，都会将系统置于一个相对容易被攻击的境地。拥有更长生命周期的系统有着比一般系统更多的潜在风险，原因是系统中的组件已经不再被原厂商以及它们的分销商生产了。因此，在无法从授权供应商渠道采购，而必须面向公开市场采购时，也有必要为此建立一套计划流程。因为作为公开市场渠道，存在的风险更大，因不合格而被推翻的风险，甚至伪劣产品，都会成比例上升[NIST 7622-2]。

5.5.3 NISTIR 7622 的应用

只要风险可以被控制和减轻，合理的冒险是合适的。本部分阐述了使用 NIST SP 800-53 在生命周期中采取措施来减缓供应链风险。NIST SP 800-53 是确定适用于信息

系统的安全控制集合(安全控制基线)的起点。并不是每一个信息系统采集都可以用来评估供应链风险或者将供应链减缓措施年纳入采购文件。对于 FIPS 199[①] 高影响的系统，ICT 供应链风险管理应该被明确嵌入到采购进程中来分析潜在的供应链风险、实施额外的安全控制并/和供应链风险管理实践;对中度影响的系统,授权机构应该做出关于是否需要 ICT 供应链风险管理的基于风险的决策;低影响系统不需要大量的 ICT 风险管理关注。如图 5-7 指出了供应链风险管理的实施流程[NIST 7622-2]。

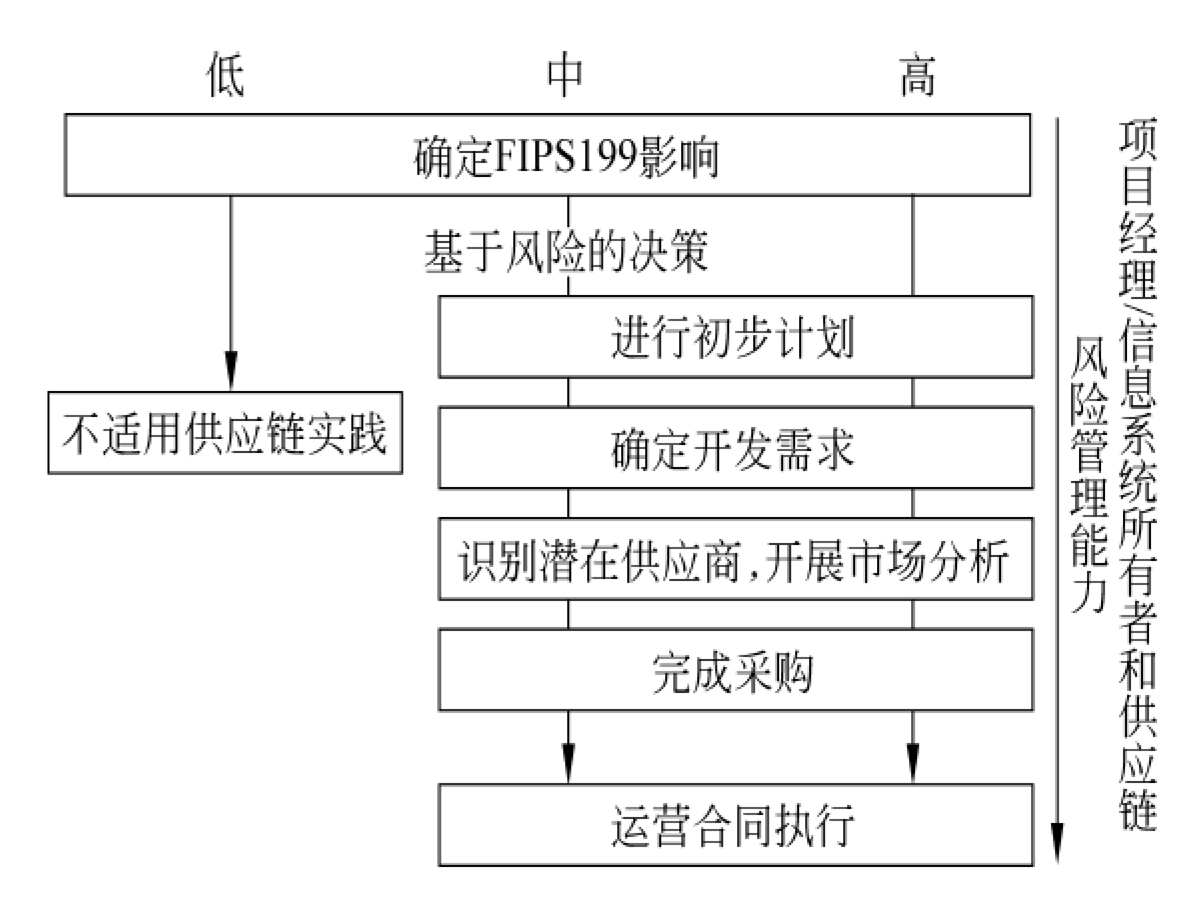


图 5-7　ICT SCRM 实施进程[NIST 7622-2]

进行初步设计：在业主或者被任命者、信息安全专家、法律顾问和 ICT 供应链风险管理团队的其他成员的协助下,采购官员应该修改或者开发出一个采购策略来最好地支持选定的项目。另外,应该透露任何法律问题,确定给政府带来最大利益的合同类型,确定完成项目需要一个还是多个集成者/供应商。

确定开发需求：系统运营方应制订工作说明书,详细说明特定技术安全需求,以及所选用的供应链风险管理实践。工作说明书要清晰明确,包括最终如何衡量业绩指标、评估标准以及临界值等。

识别潜在供应商,开展市场分析：当确定需求后,就需要寻找合适的集成商和供应商。目前有几种方式找到集成商和供应商。首先,发出招标函;其次,发出标书;随后进行市场调查,进行询价。相关主管应了解如何识别可靠的供应商(包括合格的集成商、供应商和可信产品列表)。如果不知道、或有意寻找在此之外的其他供应商时,系统运营官应与项目总监一起展开市场分析,确认什么公司可以提供需求产品,给出合格建议。

完成采购：在完成市场分析后,组织应该开发工作说明书(statement of work,SOW)和目标说明书(statement of objective,SOO)来释放请求建议书(Request For Proposal,RFP)或者报价邀请函(Request For Quotations,RFQ),如果组织发表了请求信息

---

① 美国联邦信息处理标准(FIPS)是(NIST)制定的一类安全出版物,多为强制性标准。FIPS 199《联邦信息和信息系统安全分类标准》(2003 年 12 月最终版)描述了如何确定一个信息系统的安全类别。确定系统级别的落脚点在于系统中所处理、传输、存储的所有信息类型的重要性。

信息和信息系统的"安全类别"是 FIPS 199 中提出的一种系统级别概念。该定义是建立在某些事件的发生会对机构产生潜在影响的基础之上。具体以信息和信息系统的三类安全目标(保密性、完整性和可用性)来表现,即,丧失了保密性、完整性或可用性,对机构运行、机构资产和个人产生的影响。FIPS 199 定义了三种影响级：低、中、高。

(Request For Information,RFI)或者社会保险号(Social Security Number,SSN)并据此选择了集成商/供应商的特定集合,那么这个RFP/RFQ应该发给这样的集成商/供应商群体。具体步骤包括发布建议请求/报价请求;审查建议请求/报价请求;完整的安全威胁和漏洞评估;合同谈判和授予。

运营合同执行:一旦系统可运作,操作环境可能会改变。这些变化包括但不限于供应商、元素、交付集成和商业进程。这些变化可能会修改、增加或者减少ICT供应链风险。在运作阶段,采购者应继续执行ICT供应链风险管理,包括基础企业实践的评估。采购者需要确保集成者/供应商理解供应链风险并提供关于在正在运行的基础上可应用于元素、环境、缺陷和补丁的变化的信息。

在达到以上要求的基础上,这五个过程中还应列出所有与合同相关的适用法律条文、合同类型,以及决策时有多少家符合条件供应商参加等补充内容。当供应商回复标书并提供方案时,作为技术评估组成员之一的系统运营官,应该进行技术评估,项目总监随后审计费用,来决定哪个方案的性价比最高。在进行决策前,技术评估组要检验每个集成商的供应商的方案,并衡量每份方案的质量及权重。技术评估组还应搜集集成商和供应商关于项目反馈的文档,以作为参考,如过去项目的成功比例,包括服务质量、是否正常交付、成本控制及供应商和集成商的商务往来等[NIST 7622-2]。

5.5.4 NISTIR 7622的意义

NISTIR为联邦机构提供了一套标准可行的技术和知识产权工具,来进行与其自身信息系统或网络等级相符的供应链风险管理。这套综合方法将基于政府内部专家们的努力和共识;也为所有组织提供了一套多层次的纵深防御工具集,并在签署合同时应考虑增加相关条款,来帮助企业和管理机构有效应对供应链风险。相关机构必须评估和管理供应链风险,以确保系统的正常运行。NISTIR 7622可帮助那些必须应对来自全球供应商以及有潜在威胁的企业和机构合理规划和处理管理信息采购、系统开发、系统或系统间运营中遇到的各种问题,并在控制成本、严格执行计划及满足开发需求方面有所改进。指南在系统开发生命周期中运用了一系列组合实例,以最大程度地降低供应链风险,帮助企业和相关机构应根据自身需求、计划和财务状况,选择适合自身应用的实例作为参考,从而有效规避风险[NIST 7622-2]。

参 考 文 献

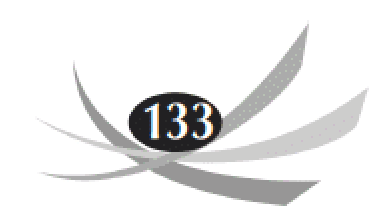
[ISO 28000] ISO. Specification for security management systems for the supply chain. 2007.

[ISO 28001] ISO. Security management systems for the supply chain-Best practices for implementing supply chain security, assessments and plans-Requirements and guidance. 2007.

[ISO 28003] ISO. Security management systems for the supply chain-Requirements for bodies providing audit and certification of supply chain security management systems. 2007.

[ISO 28004] ISO. Security management systems for the supply chain-Guidelines for the implementation of ISO/PAS 28000. 2007.

[ISO 15026:2007] ISO/IEC. systems and software engineering-systems and software assurance. 2007.



[ISO 15026-1] ISO/IEC. Systems and software engineering-Systems and software assurance-Part 1: Concepts and vocabulary. 2008.

[ISO 15026-2] ISO/IEC. Systems and software engineering-Systems and software assurance-Part 2: Assurance case. 2008.

[ISO 15026-3] ISO/IEC. Systems and software engineering-Systems and software assurance-Part 3: System integrity levels, first edition. 2011.

[ISO 15026-4] ISO/IEC. Systems and software engineering-Systems and software assurance-Part 4: Assurance in the life cycle. 2012.

[ISO 27036-1] ISO/IEC. Text for ISO/IEC 2nd WD 27036-1-Information technology-Security techniques-Information security for supplier relationships-Part 1: Overview and concepts. 2012.

[ISO 27036-2] ISO/IEC. Text for ISO/IEC 2nd WD 27036-2-Information technology-Security techniques-Information security for supplier relationships-Part 2: Common requirements. 2012.

[ISO 27036-3] ISO/IEC. Text for ISO/IEC 2nd WD 27036-3-Information technology-Security techniques-Information security for supplier relationships-Part 3: Guidelines for ICT supply chain security. 2012.

[LH2010] 陆军,胡雪梅.物流产业振兴与 ISO 28000:2007.2010.

[NIST 7622-1] Marianne Swanson, Nadya Bartol, Rama Moorthy. Piloting Supply Chain Risk Management Practices for Federal Information Systems. National Institute of Standards and Technology. 2010.

[NIST 7622-2] Jon Boyens, Celia Paulsen, Nadya Bartol, Rama Moorthy, Stephanie Shankles. Notional Supply Chain Risk Management Practices for Federal Information Systems. National Institute of Standards and Technology. 2012.

[RH] Richard Hawkins. ISO/IEC 15026 An Overview.

[SY2007] 宋扬.劳氏推出 ISO/PAS 28000 认证服务.电器.2007.

[ZT2005] 朱彤.公共标准导航 ICT 走向——ICT 产业公共标准的贸易与技术创新效应.WTO 经济导刊.2005.

[ZT2006] 朱彤.标准的经济性质与功能及其对技术创新的影响作者.经济理论与经济管理.2006.

[ZL2012] 郑兴艳,刘迎.IT 供应链安全风险管理标准研究.硕士论文.2012.

[QSQG2006] 强思企管.ISO 28000 供应链安全管理体系规范.2006.

[TJHG2011] 春雨供应链通过 ISO 28000:2007 认证.天津化工.2011.

[WZ1] http://baike. baidu. com/link? url = tOzbJ3uOy5VFkMysXPkMKAQRW _ _ 9nGr _ ABarUqfmjKQxA3CqJ5U4Vdq-EVXdJbk9XjA67cNqV9QDZdw1u_S5GJa.

[WZ2] http://baike. baidu. com/link? url = ePIu1PiqMtIc0sB7ZaGHdjuxttplpd0VNjUd2GseeZ3O-ZhpYfnjq4d17BKPXZmxA0r7glUvPvstiGlghjMzW8a.

[WZ3] http://www. lrqa. com. cn/standards-and-schemes/standards/65479-iso28000. aspx.

[WZ4] http://www. gdcoc. com/txrz/825. html.

第6章 ICT 硬件供应链安全

6.1 概　　述

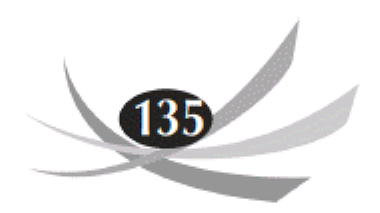
在 2004 年亚太经合组织(APEC)会议上,胡锦涛指出 ICT 改变了传统的生产方式和商业模式,为亚太地区带来了新的经济增长技术及信息通讯技术,引领可持续发展之路。在这一背景下,越来越多的 ICT 技术开始应用于企业实践,ICT 硬件供应链不断扩大。然而,ICT 硬件供应链所受的威胁也在不断增加,只有专业地保障 ICT 硬件供应链安全,才能维护我们正常的日常生活。因此,为保障 ICT 硬件供应链的安全,我们必须防止任何人为或者自然形式的破坏。

6.1.1 硬件供应链的背景

ICT 产业是一个新兴且快速发展的行业,是工业和经济发展的火车头。ICT 硬件制造业是电子行业的一部分,也是目前世界上最大、发展最快的制造业。过去的二十年中,快速发展的 ICT 部门导致电子产品的份额飙升,其份额翻了一番,在制造产品中几乎占有四分之一的世界贸易份额。但是,据研究发现,在生产中存在的主要问题是硬件。就美国而言,私人关键网络大约拥有 85%的国内重要基础设施。但美国政府对私人网络安全的保护是有限的,例如,国家网络安全部门可对关键网络的私有者提供支持和建议,但不能直接管理安全操作。为加强监管国内的重要资产,2008 年 1 月,联邦能源监管委员会发布了“强制性的和强制执行的”网络安全可靠性标准。之后,总统布什发布了网络计划,并将政府的大量焦点转向网络和信息安全。这些努力凸显了需要关注网络安全的特定资产,即网络硬件。

此外,网络作战联合职能司令部(Joint Functional Component Command - Network Warfare,JFCC-NW)提出,美国应解决关键网络中由国外制造的 IT 硬件所附带的风险,而且随着依靠国外制造 IT 硬件趋势的增长和敌方改善自己的网络作战能力,解决其网络的漏洞愈发重要。然而,我国面临同样甚至更为严重的形势。

作为潜在的最大消费市场,我国有大量的农民工供应且劳动力成本低廉,一些国外的电子制造服务公司已经将制造转向了我国,比如,一流的大型电子制造服务提供商伟创力(Flextronics)、旭电(Solectron)和捷普集团(Jabil Group)等。随着原始设备制造商和合同制造商将制造迁入我国,他们引来了许多供应商,因为我国有许多现成的低成本部件,包括电阻、电容器、开关和低端半导体等。事实上,我国现在生产了 85%的裸印刷线路板,而且组件价格比美国和欧洲的低 20%,但是半导体的生产仅限于一些低端半导体,如



二极管、模拟电路和其他离散部件。惠普公司采购部副总裁 Gerg Shoemaker 表示，尽管许多的惠普产品在中国制造，但是生产所需的高端半导体需要进口，因为中国没有许多的高端半导体生产商。究其原因，一是芯片生产不是劳动密集型的，我国在制造高端芯片时，没有较高的成本效益。二是我国芯片供应商不具有生产 90nm 高端内存的技术和设备。由此，我国急需加强硬件供应链的研究，借此来改善我国的现状[IS2005]。

据我们了解，目前国际上尚未对 ICT 硬件供应链进行明确定义。我们认为，ICT 硬件供应链，与其他类型供应链相似，是指 ICT 硬件从采购、设计、制造、组装、分配、维护到处理的一系列过程。硬件供应链包括集成电路(Integrated Circuit，IC)供应链、半导体供应链等等。任何一个供应链系统绝不是单独存在的，而是与其他系统相联系的，联系或多或少，但都不可或缺。整个 ICT 供应链中任何一环出现问题，即无论是物理攻击、盗窃，还是恐怖分子窃取供应商身份、内部人员威胁或有组织的犯罪，都将影响整个 ICT 硬件供应链安全。

2004 年，一个小短路打击了英国电讯公司，却带来巨大后果。几分钟内，13 万户电话、传真和因特网系统出现故障。31 家银行分行必须关闭，因为它们与数据中心的连接陷入泥沼，自动出纳机崩溃，即使紧急电话也不能接通。小小的短路破坏估计每天带来超过 700 万美元的损失。设想一个 ICT 系统出现故障后，将导致什么后果？

2011 年，日本地震以及泰国海啸严重影响了索尼的工厂及其供应链。其平板电视、相机、游戏机、摄像机以及 PC 业务的营利全部低于预期，直接导致当年销售跌去 10%，缩水至 810 亿美元[DBW2012]。2008 年 2 月，全球第五大电脑显示器生产商——光宝科东莞工厂发生火灾，致使该厂商单月损失 7100 万美元，甚至导致全球 PC 供应链出现紧张。同年 3 月，华硕电脑苏州工厂发生爆炸发生火灾，3 条为 IBM 代工的主板生产线被烧毁，导致损失将近 2500 万元，据分析，其损毁至少影响 5 万台服务器的出货[SINA2008]。2000 年 3 月，美国飞利浦公司第 22 号芯片厂发生了火灾，导致处理无线电信号的 RFC 芯片一下子失去了来源，由此在市场需求最旺盛的时候，爱立信公司由于芯片短缺，使公司损失了 4 亿美元的销售额，公司的市场份额也由 12%降至 9% [SINA2001]。

此外，还有引起最广泛注意的极端的供应链破坏或者紧急情况，比如墨西哥湾深海油田钻井泄漏，或者 2010 年的海地地震，致使整个地区的供应链网络崩溃。但是在日常生活中也会发生供应链破坏的情况，这些更为平常的事故也影响着物流系统和经济。平均每次因货物被盗造成的损失达到将近 4 百万美元。每年仅海盗攻击就造成全球经济 79 亿美元到 120 亿美元的损失。

以上事件，仅仅是 ICT 硬件供应链遭受攻击的例子及其导致的后果。目前，ICT 硬件供应链已变得复杂化，如一台普通的计算机可能包含来自世界各地制造和组装的组件：在苏格兰、新墨西哥或马来西亚制造的半导体芯片，在新加坡、泰国或菲律宾制造的磁盘驱动器，在日本制造的 CRT(阴极射线管)监听器，我国制造的电路板，最后在墨西哥或哥斯达黎加安装。随着这种复杂化，ICT 供应链上所遭受的攻击数量已呈指数级增长，影响也越来越大。如欧洲，每年其供应链上因偷窃所造成的经济损失就超过 82 亿欧元[PWC2011]。

因此，为确保 ICT 硬件供应链的安全，我们也必须着眼于已插入到网络中的物理硬

件——硬件组件的安全,并需要关注影响 ICT 硬件供应链安全的因素。目前,安全漏洞的硬件测试还处于起步阶段,必须改善才能满足行业需求。由此可见,保障 ICT 硬件供应链的安全至关重要。

6.1.2 硬件供应链的风险

近年来随着国际贸易的增长,ICT 硬件供应链的长度、复杂性和脆弱性也已相应增加。在 ICT 硬件供应链中,我们必须要考虑的问题如硬件组件由谁制造,在何地生产等。现在全球范围内的政府部门都开始考虑 ICT 硬件供应链对他们的 ICT 系统产生的威胁。在 ICT 硬件供应链系统与外部环境发生资源交换,以及供应链成员在协调与合作过程中,存在着各种内部不确定性和外部不确定性的风险因素,如供应、需求、生产以及物流环节的不确定性,以及对核心供应商的过分依赖、供应商数量的减少、信息共享风险和自然灾害等,即既有内部风险,又有外部风险。

外部危险包括:自然灾害、恐怖事件、突发事件等因素。

(1) 地震。地震可导致公路、铁路、海运和航空交通中断,使电子产品无法运输,从而影响交货速度。如 2011 年日本遭遇的大地震,在短期内对全球电子配件供应造成重大影响。

(2) 火灾。火灾发生的起因包括厂内的电气系统、加热器、用于生产的加热设备等。

(3) 水灾。2012 年,泰国洪水致使 10 多家硬盘驱动器工厂的正常运营遭到破坏。因泰国拥有全球四分之一的 HDD 生产规模,从而洪水严重影响了 ICT 产业供应链,尤其是 PC 供应链。

(4) 盗窃。在运输中,对库存产品的盗窃,如计算机外围设备和部件。从盗窃的角度分析,规模较小的内存芯片、处理器和消费性电子产品,对盗窃者极具吸引力[CNA]。

排除自然因素,在供应链的每个阶段,硬件供应链可能含有的内部风险如下:

(1) 供应中断,包括攻击者中断制造和交付;

(2) 错误的运输路线或延误交货;

(3) 错误的订单,如数量或项目错误;

(4) 制造的质量,即以硬件为基础引发的威胁,如硬件木马、恶意固件、伪造和劣质组件、边信道(功率损耗、时间变化、测试设施、故障、边信道间的相互影响)、克隆、逆向工程等。同时,企业也受供应商之间的质量控制问题的威胁,这进而极大地损害他们的品牌。

此外,硬件供应链还面临其他安全问题,如①违反边界的海关法;②缺少质量控制,缺乏保证质量的相关法律;③很多关于如何保护供应链硬件安全的国际协议,当代的法律、政策和标准还不成熟;④虚拟安全,如盗窃知识产权、对强加密的导入和导出、逻辑炸弹和自身更改的代码等[MHS2008]。

6.2 硬件木马

在全球化趋势和商业压力的驱使下,现代大多数集成电路都外包制造,设备制造厂也扩散到世界各地,促使 IC 供应链从高成本转向了低成本的地方,从而集成电路更易遭受硬件木马的威胁。而且,自硬件木马引起的许多军事灾难以来,这一 IC 供应链漏洞和安

全妥协已被全球所关注。本节主要讲述了硬件木马的定义、分类、风险和检测方法。

6.2.1 硬件木马的定义

硬件木马(Hardware Trojan)是硬件供应链的一种新型攻击方式,硬件木马是攻击者对电路的一种恶意更改,可以破坏计算资源的完整性、可用性,以及电子电路处理、存储或传输的信息的完整性、保密性。硬件木马可以控制、更改、监管电路的内容和通信,甚至摧毁电路。

硬件木马可通过更改专用集成电路(Application Specific IC,ASIC)、商业现货(COTS)部件、微处理器、网络处理器或数字信号处理器来实现。但目前,也有学者认为对可重复编程的IC中固件的更改也可称为硬件木马,如更改现场可编程门阵列(Field Programmable Gate Arrays,FPGA)中的比特流。硬件木马可在电路供应链的任意阶段被植入,如供应链中的概念设计、详细设计、IC布局、IC制造、测试、验证,甚至是后期制造阶段。

为提高IC的可信度和帮助定义和评测各种检测技术的能力,有必要对硬件木马进行分类。目前,流行的分类方法主要是根据硬件木马的基本特征(物理特性、激活特性、作用)将木马划分为3类,如图6-1所示[XWHS2008]。

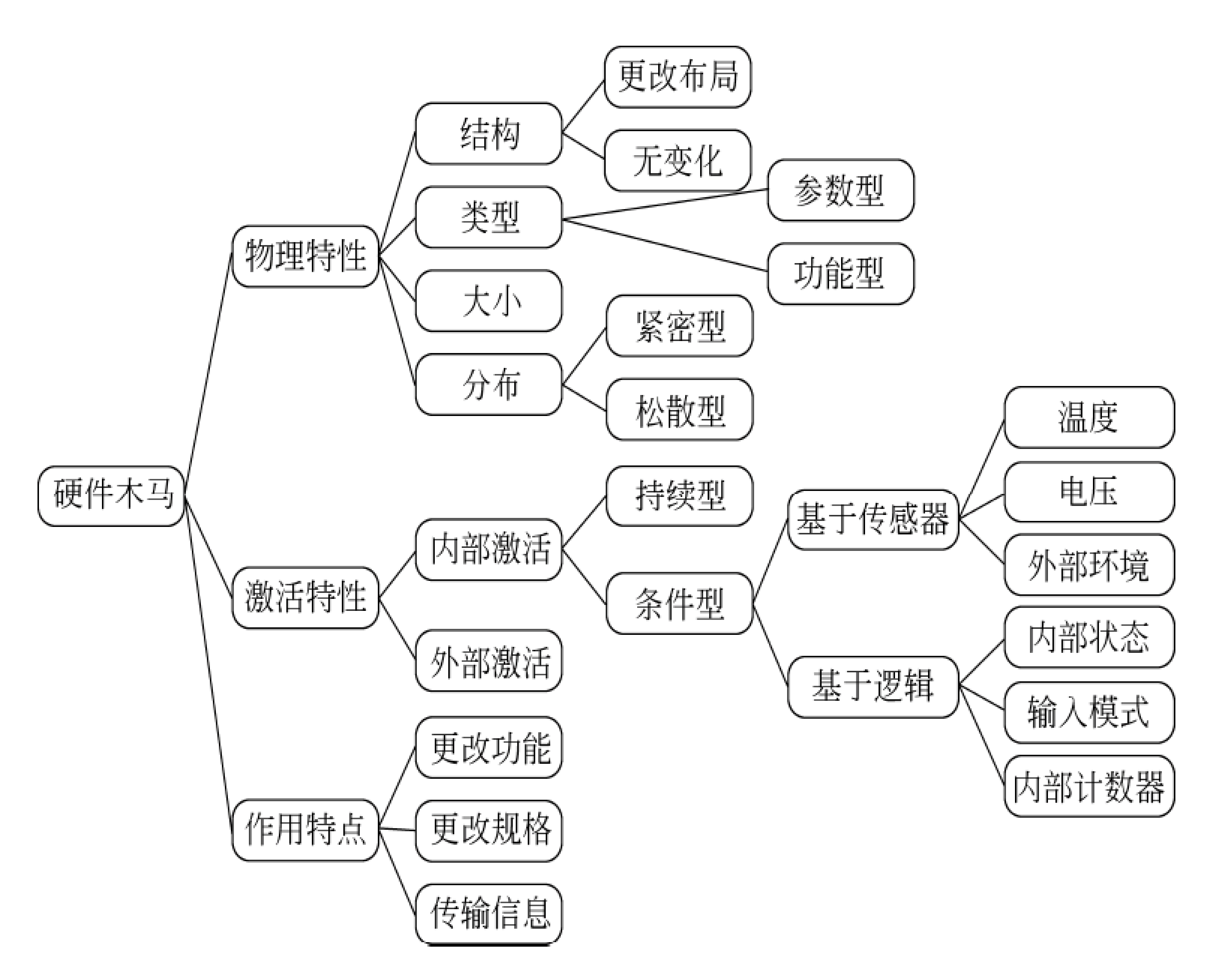


图6-1 硬件木马分类[XWMT2008]

1. 物理特性

物理特性描述了硬件木马在电路中的各种物理特征,可细分为4类:类型、分布、结构和大小。

(1) 按类型可将木马分为功能型和参数型两类。通过添加或删除晶体管或门电路实现的木马称为功能型木马,而通过修改现有的电线和逻辑实现的木马称为参数型木马。

(2) 分布类描述了硬件木马在芯片物理布局中的位置,如紧凑分布描述了木马组件

在布局中是拓扑相邻的；相对的，松散分布描述了木马组件在芯片布局中是分散的。

(3) 结构类描述了布局结构的变化。如果对手为插入木马被迫对芯片重新布局，可能更改了一些甚至所有的组件的位置，进而结构也就变化了。而且，任何物理布局的变化还可引起芯片延时和功耗特性变化，从而有助于检测木马。

(4) 大小描述了硬件木马中组件的数量或物理长度。大小在硬件木马激活时是一个重要因素，因为越小的木马比需要大量输入的木马更易激活。

2. 激活特性

激活特性指木马被激活并完成破坏功能所需的条件。为了防止意外激活和在芯片或系统测试中被检测出来，木马植入者往往设计得木马不易被用户激活。因而，从统计学的角度，木马激活事件是一种小概率事件。

激活特性可分为两类，即外部激活和内部激活。外部激活是指木马以植入者选择的方式从外部激活，可以通过往芯片中插入一个接收器或天线，后通过外部信号来控制它，还可通过访问内部寄存器，迫使寄存器在某一时间提取密钥或插入错误的处理数据。内部激活又可分为两个子类，即持续型和条件型。持续型是指木马一直处于活跃状态，可在任意时刻破坏芯片的功能。而条件型是指木马直到特定条件满足时才被激活，这种特定条件可能是基于检测温度、电压、外部环境(如湿度)的变化时传感器的输出值，也可能是基于内部逻辑状态、输入模式、内部计数器等状态来激活。

3. 作用特点

作用特性可分为更改功能、更改规格和传输信息三类。顾名思义，更改功能指硬件木马通过增加、删除或绕行现有的逻辑来改变芯片的功能。更改规格指硬件木马通过更改线路或晶体管的几何结构等来改变芯片的参数属性(如延迟)。传输信息指硬件木马从设计任务中传送关键信息给植入者。

6.2.2 硬件木马的风险

早在 2003 年 6 月，美国国会发布的关于美国半导体行业全球化给国家安全带来的影响的白皮书[JIL2003]中，就指出了硬件木马严重威胁国家安全。

2005 年，美国国防科学委员会特别工作小组在发布的关于“高性能微芯片供应的报告[DSB2005]”中指出，在军事应用中使用的非保密集成电路中，可能出现硬件木马及其他未经授权的设计嵌入。

2008 年 5 月，据纽约时报报道，联邦调查局和五角大楼称，“电子木马像邪恶的幽灵一样潜伏在计算机或网络路由器的电路中，允许攻击者秘密访问或控制设备，而且越来越多……” [MBS2012]。

2010 年，据美国国土安全部新闻网报道，戴尔公司针对硬件木马发出警告，称一部分携带多余恶意软件的服务器主板已经送抵客户。可以确认，“硬件木马”……的确是真正的威胁 [MBS2012]。

综上所述，再从 IEEE 波谱杂志(IEEE Spectrum)发布的“The Hunt for the Kill Switch”[AS2008]可以看出，硬件木马越来越引起关注。

如今，硬件木马的威胁仍在不断上升，主要源于三个因素：一是硬件的复杂性。IC

在世界各地被设计、设计部分外包或从额外的供应商购买。而且，现代集成电路设计通常涉及由第三方供应商提供的IP核(Intellectual Property Core)和由不同的供应商提供的外包设计、测试服务和电子设计自动化软件。在很大程度上，这一商业模型松散了IC设计公司对IC设计和制造的控制，从而使IC易遭受不同的安全攻击。图6-2指出了一个典型的IC生命周期中在不同步骤上的可信度。参与IC供应链中设计和制造相关的每一方都可能插入硬件木马[HT2009]。二是大多数半导体设计公司无工厂，如他们外包IC制造给不可信的外部工厂。在设计团队或恶意工厂中的恶意攻击者可以往IC中插入恶意电路[FI2013]。三是针对硬件木马的安全技术很难开发，这是因为有限的可控性和可观察性(如每个芯片中含有几万个门电路)、大规模和复杂性(如英特尔微处理器中含有十几亿晶体管)、组件的多样性、不可避免的设计漏洞、用非物理连接的电路的攻击概率、许多潜在的攻击来源(CAD工具、制造厂)、复杂的攻击者以及制造的变异性，这些都使得每个源于同样设计的IC变得唯一。据调查，硬件木马主要来源于不可信的制造厂、合成工具和库、测试和验证工具，以及配置脚本等[MP2009]。

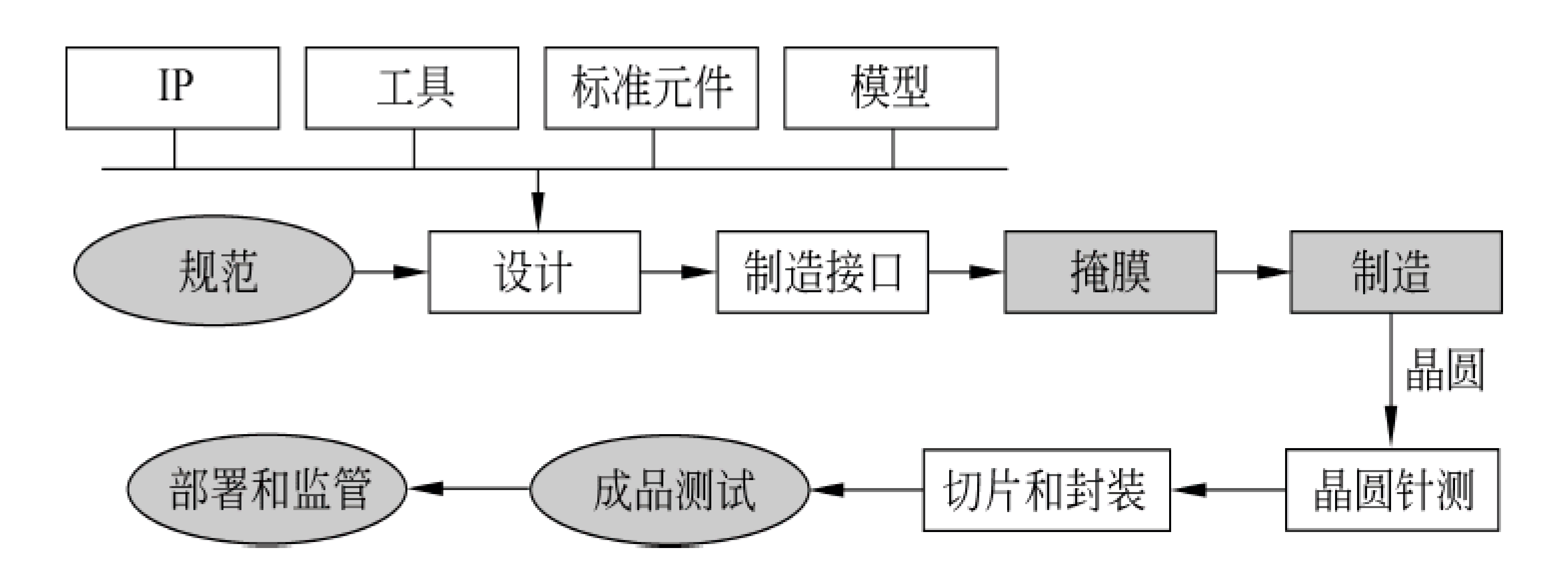


图6-2 现代IC生命周期的易受攻击的步骤(椭圆表示可信，灰底矩形表示不确定，白底矩形表示不可信)[HT2009]

目前，攻击者可能向关键系统中插入硬件木马，如军事应用(武器控制系统、战地通信系统、战场收集和信息决策系统)、航空和航天应用(航天电子设备、卫星电子设备等)、交通安全(信息管理系统、应急系统等)、大众化的关键应用系统即商业保密信息管理系统(银行系统、证券系统)和个人保密信息管理系统(医疗记录系统、个人记账系统等)。从而，对这些系统带来严重隐患。通常，硬件木马只在罕见的条件(如特定的温度或功率)下激活，正因条件罕见，所以这种木马引起的影响往往是毁灭性的。

而且，硬件木马可在将来的某一时刻被触发进而泄露机要信息(如密钥)给对手，也可能破坏芯片功能(如对微处理器的特权升级攻击)，给系统的完整性和安全性带来威胁。例如，RSA电路中的木马可能在被激活后，向RSA签名计算的反演步骤中插入故障，进而导致RSA密钥出现漏洞。

此外，鉴于硬件本身的属性，硬件木马比恶意软件更具有破坏性。首先，硬件出现了更加持久的攻击向量。一旦硬件木马对芯片作出更改，那么大量的设备(如成千上万的电子口令卡)将被影响。相对于软件可以通过打补丁或重新开发来修补漏洞而言，这种硬件级的漏洞很可能无法修复，进而需要更换该硬件组件。如今，回收一个硬件需要耗资数十亿元，例如英特尔因奔腾浮点除错误(Pentium FDIV Bug)耗资5亿美元回收500万芯片。此外，更换硬件要求的高技能和嵌入设备的使用率上升促使了即使在漏洞发现后，脆弱性系统仍将

继续使用。其次,硬件是计算机系统的最低层,可提供给恶意硬件的控制权力多于软件的权力。这种低层次的控制使先进的隐身攻击可规避软件的防御[MH2010]。总之,硬件木马已成为各类安全模块的重要威胁。

6.2.3 硬件木马的检测

鉴于硬件木马可对系统产生巨大破坏,在硬件供应链中及时检测硬件木马就显得非常重要。但是,检测电路中的硬件木马面临巨大的挑战。

(1) 系统级芯片(SoC)使用了大量的 IP 核且知识产权具有高复杂性,从而极难检测芯片中小型的恶意更改。

(2) 纳米集成电路特征值和系统的复杂性使得物理检查和破坏性的逆向工程检测非常困难,而且成本较高。此外,破坏性的逆向工程并不能保证无损检测的 IC 是无木马的。并且,对手可能在大批装配式芯片中随机地插入木马。

(3) 木马电路只在特定条件下激活,很难使用随机激励完全激活它们,而且很难使用观察点(主要的输出值和扫描触发器)来检测出它们。

(4) 随着工艺、光刻、环境的改善,物理大小对电路参数的完整性影响越来越大。因而,检测木马只使用简单的参数分析是无用的[MT2010]。

(5) 传统的测试方法对检测硬件木马几乎无用[YJ2009],原因如下:

① 故障列表中不包含非预期的行为,例如结构模式测试很可能没有涵盖木马测试向量。

② 不知道攻击者插入木马,很难预测真实设计中的额外的恶意功能。因而,常规功能测试无法发现有害的多余功能。

③ 详尽的输入模式测试是不切实际的,因为伴随大量的主输入和内部关口,芯片已变得越来越复杂。

④ 用于检测制造缺陷的测试(如延迟故障)无法保证木马的检测。如自动测试模式生成(Automatic Test Pattern Generation,ATPG)方法通过操纵无木马电路的网表来检测缺陷,因而无法激活和检测木马。即使对于所有类型的制造故障可能有 100%的覆盖率,也无法保证电路中无木马。

尽管通过常规的功能检测技术很难检测出硬件木马,但是目前也已开发出了许多的针对芯片级和架构级的木马检测和防范方法,对此提出了多种分类方法,既可分为边信道分析和木马激活[MT2010],也可分为故障分析方法、基于 ATPG 的检测方法和边信道分析方法[XWMT2008]。我们认为,后者划分更合理些。

1. 故障分析(Failure Analysis-based Techniques)法

故障分析需要使用先进的分析技术,如扫描光学显微镜(Scanning Optical Microscopy,SOM)、扫描电镜(Scanning Electron Microscopy,SEM)、电压对比成像(Voltage Contrast Imaging,VCI),甚至是微秒成像电路分析(Pico-second Imaging Circuit Analysis,PICA)等。尽管这些技术对认证非常有效,但是它们极其耗时,代价较高。该测试非常依赖于实验仪器,而且无法应用于运行的集成电路。该方法也不适用于每个芯片都需要认证的应用,且越来越不适用于纳米级领域。由于对手可能随机插入木

马，在认证每个芯片时花费大量的时间并不可取。所以，仍然需要高度可信且耗费较少认证时间的木马检测方法。

2. 基于ATPG的检测方法

基于ATPG的方法需要使用标准的超大规模集成电路错误检测工具(如ATPG)生成测试用例，通过应用数字激励和检查芯片的数字输出来检测恶意硬件所带有的非预期功能。数字激励是使用芯片的网表派生出来的，但是对于参数型木马，无论芯片中是否含有木马，网表都是相同的。这是由参数型木马本身决定的，因为它是通过在现有的芯片逻辑中违反设计原则实现的。因此，针对参数型木马，ATPG需要更改才能使用。考虑到秘密激活条件，针对难以检测(如不易控制或观察)的节点和路径进行生成测试，ATPG可能很有效地激活和检测木马。而且，在工艺变化和测量噪声的影响下，该方法仍然非常可靠。

但是，该方法既无法检测复杂的触发模式或隐藏方式的木马，也无法检测功能型木马。因为，不了解功能型木马的逻辑，也不知该逻辑和芯片的原始逻辑的联系，ATPG无法针对引起激活的向量或状态进行特定搜索。如果可以确定激活条件，然后猜想木马更改初始的状态或芯片的输出，尝试进行多次检测。然而，数字测试方法无法检测由边信道引起的激活或泄露信息的木马。但是，边信道分析可以解决这些问题。

3. 边信道分析方法

边信道分析主要是通过多种模拟测量来描述集成电路，例如功率跟踪或内部延迟，然后根据可信IC的描述来分析可疑的IC。边信道方法属于IC认证的一种有用技术。基于功率的边信号提供IC内部结构和活动的可见性，但是使用木马检测并没有完全激活它们。基于时间的边信道分析可使用对电路延时变化敏感的延时测试来检测是否存在木马。例如，基于指纹的边信道检测方法不需要改变目前的IC设计和制造过程，也不需要可信的制造厂。但是该检测方法需要可信的IC测试设施来生成指纹并验证，以此来保证IC中出现木马的概率非常小。对IC中的边信道信号(如功率、温度)使用噪声建模来构造一系列指纹。指纹方法：首先从全体IC中随机选择几个IC，后对该IC集进行充足的I/O测试，并收集其边信道信号。然后再利用边信道信号构建全体IC的边信道指纹，再对选定的IC集进行破坏性测试以验证它们符合原始的规格。若测试后未发现问题，则对剩余的IC用同样的I/O测试进行非破坏性测试，以检验它们的边信道信号与全体边信道指纹中的是否相一致，从而判断有无木马[DA2007]。

从理论上讲，边信道分析可应用于所有运作模式、任意大小和复杂性的木马。但是边信道分析方法也具有局限性，首先，对手利用几个逻辑门制造非常小的木马，这种小木马对电路功率产生很小的影响或延迟。因而，可以很容易地逃过边信道检测。其次，电路的特性值极易受到工艺变化和测量噪声的影响。目前在工艺变化中，即使最先进的降噪声技术也无法任意检测出小木马。最后，边信道分析允许从电子设备内部的物理信道中提取信息，目前已有证明即许多其他物理属性(如时间、声波)会泄露可用信息[LL2009]。

此外，木马检测方法也可根据对芯片有无损害来划分，即破坏性检测和非破坏性检测(如边信道分析检测方法和基于ATPG的检测方法)[RS2009]。在破坏性检测方法中，制造的IC是层层检查，通过先进的软件集成和分析这些层的芯片显微照片，以检测是否

有篡改。尽管该方法在检测芯片的完整性和真实性时仍然有效,但是它也有局限性,因为黑客很可能更改生产线中一个小的随机芯片样本,这意味着检测木马的成功完全取决于正确的选择已实际篡改的IC用例,进而该方法无法保证未测试的芯片是安全的。而且,验证IC的破坏性方法代价很高,如验证单个IC可能用几个月,成本高而且需要先进的现代化技术。因而,研究需着重于有效的无损检测方法。

近来,出现一种新兴的IC制造技术即三维(Three-dimensional,3D)IC技术,该技术可用来抵御往制造设施中插入木马。通过在不同的制造中制造3D IC中的每一层,通过混淆设计意图,从而提高安全性。即3D IC由2个或多个独立制造的IC组成,将IC垂直排列,每个IC可视为一层。通过硅通孔(Through-silivon Vias,TSV)实现层间的交互。因为在每一个IC都在单独的制造厂制造,在安全设施中垂直排列,所以无论哪个厂中的恶意攻击者都不知道整个电路图,降低了攻击者更改电路功能的可能性[FI2013]。

此外,国外一些著名的大学也在积极研究检测硬件木马的方法,如卡内基-梅隆大学有学者曾提出一种基于随机的概率方法来检测木马电路。该方法是概率比较设计的电路的功能性。如果实施电路被感染,则表明电路中存在木马,还可用指纹输入模式来区别设计和实现电路[SJ2008]。

尽管如此,依靠现有的这些检测方法是无法检测出商业现成的IC中的所有的硬件木马,对此有学者提出用逆向思维方法,即假定硬件是污染的,试图在任何未知硬件木马都出现的情况下仍能安全操作。通过采取一种深度防御的方法来对抗硬件木马,并基于分散执行和复制提出了几个模型系统。这些系统可结合多中央处理器和最小信任逻辑来对硬件木马进行抗性计算。分散执行涉及程序中使用不同的CPU时分复用以尽量减少任何单个CPU可以访问的数据量。而且,所有的计算都可跨多个CPU来复制以提高计算的完整性。

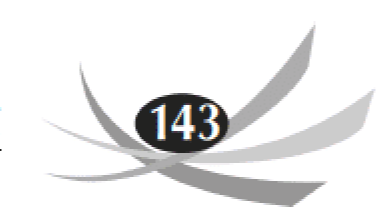
总之,硬件木马还是一个较新的研究领域,相关检测技术目前还不够成熟,对该领域的研究还缺乏大量数据,于是成熟完善的检测方案亟待出现。

6.3 恶意固件

2008年,惠普公司的研究员Rich West在欧洲著名安全会议EUSecWest上曾表示,网络连接存储、网络及安全设备可通过下载恶意固件及接入闪存装置而轻易地遭受攻击,致使硬件无法工作[QYW2011]。显然,硬件无法工作,将使产品在使用阶段造成ICT硬件供应链中断。本节主要讲述了恶意固件的定义、风险和检测方法。

6.3.1 恶意固件的定义

固件是写入可编程只读存储器(ROM)或闪存中的底层软件,简言之,固件即固化的软件。固件的主要功能包括:功率自检、启动设备、提供运行时服务、设置和存储配置数据、加载操作系统并担任硬件和操作系统间通信的桥梁。对于某些类型的硬件,固件由设备制造商设定,且不会更改。网络外设的用户和终端用户可通过制造商和供应商下载,进而更新固件版本。在某些情况下,固件提供给操作系统一个接口,以致操作系统能操作该



设备。在其他情况下，固件在设备启动引导过程中执行，例如，BIOS 在加载操作系统(OS)前运行。其他固件(可选 ROM)居留在外围设备中，允许操作系统有效地使用该设备。

与普通软件一样，固件也可能存在后门、逻辑炸弹、木马、蠕虫等具有恶意行为的代码。含有这类恶意代码的固件称为恶意固件。恶意固件采用同恶意软件一样的方式运行。如果含有恶意固件的电子组件接入攻击者可以访问的任意网络，恶意固件会将信息系统的控制权交给攻击者，后果不可设想。为加强对固件的了解和控制，希望尽可能了解固件的恶意行为。但是对于恶意固件中程序的恶意行为，传统的程序恶意行为描述将不再适用，因为固件是固化在底层硬件内部的程序，与硬件密切相关，且它以特权方式运行，具有代码执行的阶段性和高内聚性等特点。

6.3.2 恶意固件的风险

近来，有研究表明，在典型的 x86 计算机系统中，恶意软件可利用固件本身或固件升级工具的脆弱性感染外围设备的固件[YL2011]。

2009 年，佐治亚理工学院的 K. Chen 证明了利用苹果键盘固件升级工具中的漏洞，攻击者可在固件升级时向苹果键盘中插入恶意代码(如键盘记录器)，从而使主机 OS 带有漏洞[KC2009]。

2010 年，在博通公司的 NIC(Network Controllers)固件中，发现了一个缓冲区溢出漏洞，该漏洞可使远程攻击者通过发送恶意包给 NIC，然后执行 NIC 中的任意代码，进而损害 NIC 固件[LD2010]。

2012 年，安全研究员 Jonathan 在黑帽大会上创建了一个概念验证的硬件后门，命名为 Rakshasa。Rakshasa 采用了 iPXE 固件(iPXE 是一款开源的网络引导固件，是 PXE 的改进，用于远程加载操作系统)，通过远程下载 bootkit 后潜入系统，电脑启动时将其加载到 RAM 中，进而置换电脑上现有的主板 BIOS，并可感染其他外围设备(如网卡、CD-ROM 等)上的 PCI 固件，从而在引导时，不留痕迹地损害 OS。

2013 年，Clear Hat Consulting 公司的 Sherri Sparks 在 DHS S&T/DoD ASD (R&E) CYBER SECURITY SBIR WORKSHOP 上表示，大多数商业硬盘驱动器在固件开发方面具有脆弱性，而目前的安全产品并没有解决这些脆弱性[SS2013]。

而且，同年还发现，Linksys 的 WRT54GL 路由器中含有跨站请求伪造(Cross Site Request Forgery)漏洞允许对任意的固件进行非认证更新[DS2013]。

最近，互联网安全联盟(Internet Security Alliance，ISA)发布的保护电子供应链的报告[SB2013]中指出，对包装的产品进行随机测试并采取预防测试，以确保含有恶意固件的电子组件不进入下一测试领域。

可见，如今固件已经成为了供应链中一种不可忽视的威胁，例如，智能电网信息系统中的固件组件的变化可能影响整个系统的安全。而且，目前感染的固件正越来越普遍，如许多 DVD 播放器已经破解固件来支持任意领域的 DVD[JH2004]。究其根源，固件与硬件电路相比，其安全性更差，因为恶意的经销商可通过病毒等更改固件，而在硬件电路中，掩膜组的研发比较昂贵，专门针对研发的风险较少。与软件相比，固件比较单一，而且大

多数的编程人员不熟悉固件,对固件的安全意识较差,进而攻击者更改固件的难度低于更改 OS 代码,这潜在地造就了固件攻击最大的脆弱性。

目前,根据发现的固件缺陷和攻击,可将固件的风险分为三类:

(1) 固件本身含有漏洞,例如,最近美国国土安全部发布警告,称在工业控制系统中发现某些固件含有漏洞,攻击者利用这种漏洞发动一种拒绝服务攻击,修改模块的内存和执行任意代码[GAO-12-361]。

(2) 固件更改攻击,可通过利用嵌入式软件的设计缺陷、无授权认证的固件更新来破坏设备的固件。固件更改攻击可以影响带有同种系统设计缺陷的整个设备系列。据了解,目前可对通信设施、笔记本的电池控制器、ATM 等进行固件更改攻击。例如 2004 年,在雅典奥运会期间,攻击者通过更改沃达丰(Vodafone)爱立信交换机(Ericsson AXE)上控制器,将需要监听的数据流传送给若干台“影子手机”,该事件导致希腊总理夫妇在内的至少 100 个政要的通话被窃听,因此沃达丰被罚款约 8 亿元人民币。2010 年,在黑帽大会上,Barnaby Jack 通过更改两台 ATM 机中的固件,控制 ATM 取款机自动吐钱。

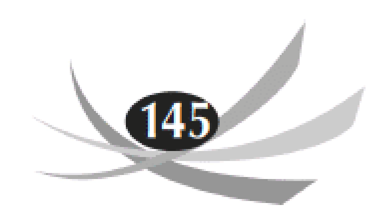
固件更改攻击的影响可分为两类,一类是攻击者破坏固件的完整性和可用性,这是一种拒绝式服务攻击,将导致设备无法正常加载等。另一类是攻击者插入恶意代码后,系统仍可用,但是将存有隐患。例如,BIOS 的代码或配置被恶意更改后,可致使计算机丧失保密性、完整性和可用性,引发系统的不稳定性、系统故障和信息泄露。而且,计算机将易于遭受更复杂的攻击,如秘密监视,还可用作攻击其他系统的垫脚石。固件攻击甚至可以削弱最复杂的应用层控制或安全机制。如果底层固件不可信,那么操作系统和应用层安全机制也不可信。近年来,对于 BIOS 攻击和威胁事件不断上升已证实了这一点。

(3) 固件的认证技术尚不成熟。固件通常存储在驱动器的不同区域(如磁盘盘片和序列式闪存(Serial Flash)),访问这些不同的区域比较慢,而且具有不同的时间延迟。现有的软件认证技术通常认为这种时间延迟是难以预测的,所以对固件的认证还是比较困难的。例如,目前对固件采取的安全性措施即实施固件签名。但是签名的固件仍无法阻止攻击者用相似的固件来替换。因为近来发现,数字签名机制在哈希碰撞、验证授权和软件供应商证书方面含有漏洞。而且,固件签名仅在加载时检查代码的完整性,无法阻止运行时更改攻击。例如,ATA 总线中的固件漏洞允许感染驱动和绕过签名更新机制。此外,由于目前在硬盘中没有相关的防范技术,所以这种漏洞还很容易被利用。

恶意固件往往带有其他附加的问题,例如,恶意固件可使 ICT 硬件供应链中断,从而企业因其供应链的中断的威胁而导致生产延迟,极大地增加了他们的成本。因此,解决恶意固件问题对保证 ICT 硬件供应链安全具有重要意义和作用。

6.3.3 恶意固件的检测

随着固件入侵事件的增多,非常有必要检测固件系统。早在 1982 年,HELMUT K. BERG、PRAKASH RAO 和 BRUCE D. SHRIVER[HB1982]就提出了固件质量确保。他们认为,固件系统需满足功能、性能、操作和实现属性。但是目前,对固件的安全保护面临许多难点,例如因为设备的成本较高,所以基于硬件的保护是不切实际的。而且,现未



有一种统一的固件检测系统来检测固件是否是恶意的。检测外围设备上的固件也是一技术难题，已在2013年乔治亚技术信息安全中心(Georgia Tech Information Security Center)发布的新兴的网络威胁报告中指出了，目前依然很难检测固件的变化[GTISC2012]。这是由于恶意软件检测机制、二进制分析等因外围设备的有限内存、计算资源和处理等局限性而不适用于外围设备固件的检测。因而，需要思考新的检测策略和部署工具。据我们了解，现有的检测方法有：

(1) 可借助于总线海盗来检测固件。总线海盗是一个开源的电子元器件测试与开发工具，它将常用的电子设备通讯总线集成在一起，方便开发人员快速的测试项目原型。

(2) 通过供应链检测固件所受的攻击，该方法往往是分析设备或设备的行为。佐治亚理工学院的研究人员正在探索更加有效的策略，设法证明信息系统中的基本组件的可信性，以致更改(即使在制造过程中被更改)都可以检测。类似于开发适用于Windows 8的安全引导技术，该技术可阻止更改计算机系统中的固件，并有助于确定系统中软件是否仍然可信。

佐治亚理工学院的研究员Andrew Howard表示，问题在于我们是否可以向设备中加入隐藏的功能来确定该设备是我们自己的设备。其他方法包括使用无损检测识别组件签名，并检测与已知组件信息不匹配的组件，或检测与伪造组件信息匹配的组件[GTISC2012]。

(3) 可信测量核心根(Core Root of Trust for Measurement，CRTM)，针对可行根的攻击，采用可信测量的核心根来保护其免受远程攻击。然而，它本身无法规避供应链攻击。该方法使用硬件、固件和软件工具来检测供应链攻击。该方法由可扫描闪存内容的硬件头和可计算被扫描的固件中的hash的软件工具组成，并通过使用扫描代码的hash和golden hash来定位固件攻击。该系统使用现有的CRTM特性和安全的引导特性来检测整个固件栈中的固件攻击[IPPAD2013]。

(4) 机器学习法，旨在恶意检测器不停地监管系统中的各类特征和事件，后应用标准的分类器来分类收集的观察结果得出正常或恶意的。分类方法可以使用K均值、直方图、决策树、贝叶斯网络等。评价机器学习分类器可分为两个阶段，即训练和测试。在第一阶段，将特征向量的测试集提供给系统。通过系统正常运行时表现的行为和恶意软件激活时表现的行为来收集特征向量。在训练集中有代表性的特征向量和每一向量的真实分类被认为是学习算法，该算法生成训练分类器。在测试阶段，通过训练分类器划分良性和恶性特征向量。在测试阶段，分类器的性能通过提取标准的评价测试措施来评价[AS2012]。

尽管目前的认证方法可检测针对OS、BIOS和可选的ROM攻击，但是对其他恶意固件的检测可能则不再困难了。可直接访问内存的固件的危险不亚于BIOS或内核的危险，即使不直接访问内存的固件也可能需要信任。因此，尽管外围设备和内存隐含的被认为是TCB的一部分，但是这种可信性还需亟待验证[JH2004]。

总之，目前对恶意固件的检测还不理想，仍需很长的一段路要走。在此，简单提及两种防御方法，一种是通过数字签名、监管链和物理保护来保证固件的完整性。基于对供应商和一些代码的详细审查的信任，该策略的初想是固件初始是完好的。该策略只能保证



已被认证的代码没有被更改。但是该策略的实施成本较高。因其需建立一个大而广泛的可信供应商的网络。而且，具有通过互联网，自动更新设备驱动程序和固件补丁的机制。固件的常规更新每次都需要再检查。

另一种是固件保护模式，即(1)对固件的引导增加安全措施，如用U-boot验证Linux内核签名。(2)用固件测量，我们可以检测供应链或其他固件更改。(3)用硬件保护模式(Hardware Protection Mode，HPM)封锁，即使在远程攻击者获取root密码的情况下，仍可以保护固件免受远程更改。(4)通过对更新进行RSA签名，在认证固件签名通过的情况下，才对固件进行更新，从而确保更新安全[DS2013]。

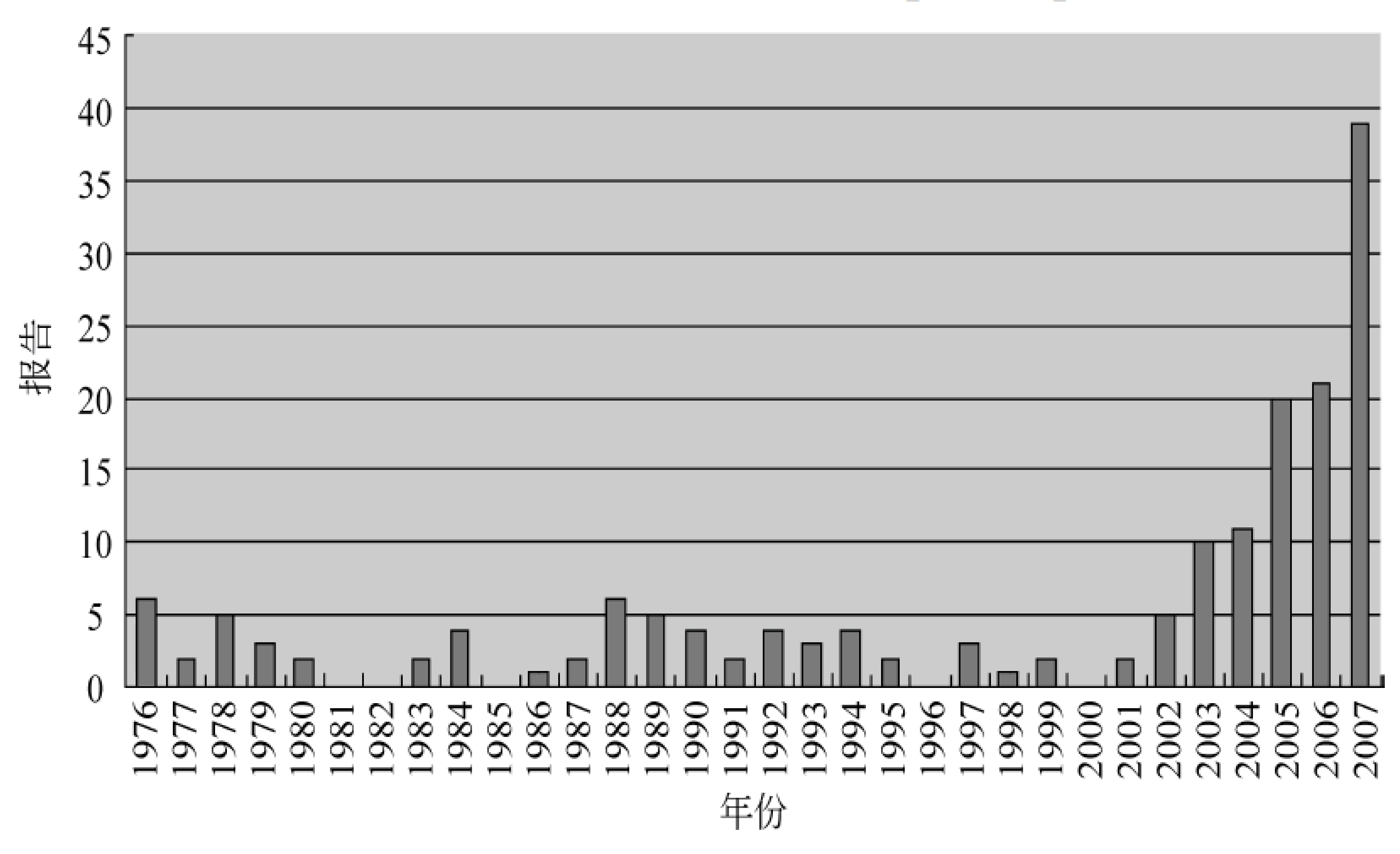
6.4 硬件伪造

近年来伪造事件不断发生，伪造元件也以惊人的速度渗入ICT供应链中。这一恶化事实如下。

(1) 2005年，美国国防部技术评估办公室(OTE)从387家美国公司的供应链(从零部件制造商到总承包商)中采样，寻找伪造的微电路、电路板和离散电子。OTE在政府的敏感武器和通信设备部门采购的电子配件中发现了3868起伪造配件事件。2008年，OTE重复采样，发现了9356起类似伪造事件。

(2) 2007年11～12月的3周内，美国海关边境保护局(CBP)和欧盟海关实施“运营基础设施”行动，查获了36万套伪造集成电路和计算机网络元器件，这些伪造组件涉及了40种不同的商标[CBP2008]。同年，GIDEP给出的关于伪造电子组件的报告中给出的数据，如表6-1所示。

表6-1 关于伪造电子组件的报告[BH2008]



(3) 从2007年至2010年之间，美国CBP与移民海关执法局(ICE)共同查扣约1300多件伪造半导体元件，价值高达560万美元，其中一半以上的伪造元件中还不实地标记着航空级或军用设备。

(4) 2010年，ICE查扣的最多商品之一是伪造的电脑硬件(包括芯片)。ICE在报告中指出，这部分被查扣的商品比2009年增加了五倍之多。同年，美国商务部对国防

工业中的伪造电子产品的研究也证实了这一趋势。而且，商务部根据原始元件制造商(OCM)的回应发现，在2005—2008年间，政府和军事应用中的伪造元件增加了1.5倍以上。

(5) 2011年，美国GAO发布报告称，伪造元件的不断增长，是国防部解决质量问题时面临的重要阻碍之一[GAO-11-404]。同年，市场研究机构iHS iSuppli称2011年是伪造电子元器件创纪录的一年，有记录的伪造案件1363起，是2009年的4倍。并且，过去5年来有近1200万个仿冒元器件被发现，即平均每15秒就产生1个伪造元件，这对全球供应链产生了致命的影响[IHSO2012]。

(6) 2012年，GAO发布报告[GAO-12-375]称，在互联网采购平台上可以发现伪造电子元件。同年，iHS iSuppli发布报告称，全球五种最常见的伪造半导体产品(模拟集成电路、存储器、可编程逻辑集成电路、微处理器集成电路、晶体管)对全球电子供应链带来年度达1690亿美元的潜在风险[IHS2012]。

(7) 2013年，威瑞信公司(VeriSign)发布的关于网络安全威胁的白皮书《2013 CYBER SECURITY DISRUPTORS AN OVERVIEW》中指出，据估计，市场中有十分之一的产品是伪造的[VeriSign2013]。

6.4.1 硬件伪造的定义

在2010年，全球主流IC产品出现了产能紧张、供不应求、交期延迟的现象，而为满足生产线所需，不少买家寻求除授权分销商外的供货渠道，进而伪造品、翻新货等名词再度活跃于市场，导致很多人在不知情或图便宜心理下深受伪造电子元件的危害。据美国联邦机构估计，全球电子供应链的10%到11%是假的——从iPad和iPod到路由器、交换机等等都会有伪造品。那何为伪造组件？何为非伪造组件呢？

(1) 就非伪造组件而言，BAE系统公司给出了如下观点：

- 为支持装备的可生产性和保证设备可靠性的再加工零件。
- 为满足客户需求进行再审查的元件。
- 改善一些部件来满足超出制造商规定的应用范围的性能需求。

电子产品制造商和政府用户使用这些方法来确保组件满足设备性能和可靠性的需求。

(2) 对于伪造组件：

① 从航空和国防设备制造商的角度，伪造电子组件通常指给政府设备制造商和用户带来风险的组件。例如：

- 标记产品，以掩盖不同于原始组件制造商制造组件的部分，如原制造商、原产国、特定的性能等；
- 由原制造商报废的缺陷零件；
- 使用废弃的装配组件。

这些都危及电子组件的可靠性和性能。

② AIA CP-IPT 对伪造品的定义。

美国航空航天工业协会(Aerospace Industries Association,AIA)的伪造集成部件项目组(Counterfeit Parts-Integrated Project Team,CP-IPT)定义产品伪造为误传货物来源或性质,既包括假商标、服务标志、原产地标签、认证标志等,又包括非法模仿他人生产的受版权或法律保护的商品包装[AIA2011]。

③ SIA ACTF 对伪造组件的定义。

2006 年 6 月成立的美国半导体产业协会防伪特遣部队(SIA ACTF)定义伪造组件为:替代产品或未经授权的复制产品;除了原始的产品制造商外,更改产品的使用材料或改变产品性能的产品;以及供应商提供的劣质产品。

④ OTE 对伪造品的定义。

OTE 对伪造品定义比较宽泛,该定义包含了供应链不同阶段的观点。伪造品指一个不地道的电子产品,即未经授权的抄袭产品,例如没有管芯的空封装;不符合原始部件生产商(OCMs)的设计、模型和性能标准的产品;不是由原始部件生产商生产,而是由未授权的承包商生产的产品;是不符合规范的、有缺陷的或者将用过的原始部件生产商的产品经过翻新后得到的产品;提供错误的标志和证明文件,比如故意标高速率等级和温度等级,使得用户将消费级芯片用于工业级[USDC2010]。

6.4.2 硬件伪造的渗入

目前,遭遇的伪造组件的主要类型包括:①供应商谎称源于一个特定制造商的部件;②故意不包含预订部件中的合适的内部部件或构架的部件;③不如实标明使用年限和修理年限的真实部件;④伪造包装的部件。这些伪造组件如何成功渗入 ICT 硬件供应链呢?就美国而言,其国防部对伪造的调查报告[USDC2010]表示:

(1) 国防供应链中各个组织之间缺乏关于伪造品的交流。5 个领域(OCMs、授权和未授权的零部件供应商、电路板组装商、主承包商和次级承包商以及国防部)的调查数据显示,各个组织通常只在各自内部讨论伪造品问题,与他们的客户和中间供应商的讨论范围较小。这导致整个供应链中降低伪造品风险的分享信息缺失。

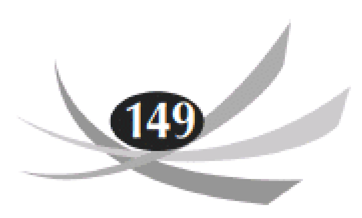
(2) 经常认为供应链中其他成员会检测零部件。各个领域中的组织都依赖供应链中其他成员来测试和验证零部件的真实性和可靠性,因此自身进行较少的测试。但是从调查的数据来看,这种对于其他组织会测试的信心是毫无依据的。

(3) 供应链中缺少可追踪性。采购组织经常不能有效地追踪到所购产品的原始生产者。许多元件由海外的供应商提供,让生产者的认证变得更为困难。

(4) 组织内部的不充分问责链。很少有调查参与者能确定一个指定的人员或者办公室需要对伪造品带来的风险负责或应由谁处理伪造品零部件。这将导致组织内部缺乏集中的数据和缺少一致的预防伪造品措施。

(5) 各个组织缺乏对于伪造品事件的记录。大部分的组织没有记录伪造品事件。即使有的组织记录也只记录有限的信息。因而缺乏制度化的记录一个组织遇到的伪造品问题及采取的措施。

(6) 当遇到伪造品时,不知道该与谁联系。OTE 的分析者指出,国防部的刑事调查



服务(DCIS)和联邦航空调查局(FAA)是联邦政府中各自负责国防和商业航空领域伪造品的政府部门。然而,分析者不能清晰地指明哪个政府部门负责与商业产品相关的伪造品(包括支持重要基础设施的零部件),或者指出与处理供应链中伪造品相关的法律要求。

(7) 很少有调查对象了解伪造品相关的法律要求和责任。参与调查的大部分人员并不知道与伪造品管理、分销、储藏和弃置相关的法律要求和责任。

(8) 需要更为严格的测试程序和质量控制措施。各个组织购买和得到零部件时,进行的测试水平和质量有十分大的区别。而且,目前不存在第三方测试设施的标准。尽管目前有行业标准来应对测试和质量控制问题,但是这些标准并没有被供应链系统所采用和实施。

(9) 大部分国防部组织没有现存的防止伪造零部件渗入他们的供应链的政策。国防部组织倾向于依靠国防部联邦收购条例(DFAR)来指导他们的采购实践。在其调查期间,很少有组织制定额外的采购和测试程序来应对伪造零部件所引发的问题。

例如,电路板组装商提供了几个伪造品进入美国供应链的原因。大多数的组装商指出较不严格的存货管理和更多的依靠未授权经销商的灰色市场是重要原因。组装商也指出不足的零部件生产,不足的零部件生产终结告知,原始设备制造商不足的零部件购买计划,不足的责任制也是原因之一。电路板组装商指出的伪造品进入供应链的 10 大原因如表 6-2 所示。

表 6-2 伪造品进入供应链的原因[USDC2010]

组件经纪人对库存管理较松	63%
组件经纪人较多的依赖于灰色市场零部件	59%
开放市场上过剩库存的购买	50%
独立经销商较多的依赖于灰色市场零部件	47%
原始组件生产商生产不足	44%
零部件生产终结告知不足	44%
原始设备制造商零部件购买计划不足	41%
独立经销商较松的库存管理	38%
责任制不足	38%
合同制造商较多的依赖于灰色市场零部件	31%

6.4.3 硬件伪造的根源

由于政府监管及产业本身的漏洞,伪造电子元件越来越泛滥,可谓在电子元件供应链中无所不在。ICT 行业在试图消除伪造元件带来的恶劣影响时需要付出更多的努力。但如若找到伪造硬件的根源,努力从根源减少或消除伪造元件,可起到事半功倍的效果。

1. 短缺元件

伪造者实时关注市场需求,准确地掌握着元件市场的情况。在半导体及电子元件中,

伪造者不仅会轻易盯上某些产品，如供货量大且单价高的微处理器、因产品等级不同而存在较大价格差别元件，而且会盯上那些需求紧迫但处于缺货状态的产品，即短缺元件，因为短缺元件一般包含一些过时的元件。过时的元件市场对伪造者特别有吸引力，因为元件越难找到，其获取的利润越高。尽管设备厂商一般通过正规销售商来采购半导体及电子元件，但由于从正规的销售点采购比较困难，为能按时完成生产而拼命采购部件的设备厂商，会从网络销售商等“开放市场”获取短缺元件。这时供应商就会面临买到伪造元件的风险。

2. 根源在于电子垃圾

工业研究发现许多的伪造电子组件源于从海外部分地区回收的电子垃圾。而且，IHS 供应链高级总监 Bob Braasch 表示，大部分伪造元器件的问题根源于每年产生的大量电子垃圾。电子垃圾是由丢弃的、新的或旧的、功能性或非功能性的电子设备或组件组成的废弃物。随着全球经济发展和技术的进步，消费者越来越追求最新的科技产品，而过时的电子产品则变成了电子垃圾。出口到发展中国家的电子垃圾和废料正是伪造者制造电子部件的“原料”[HL2010]。

并且，电子垃圾是一个快速增长的问题。2002 年，在美国，估计有 1275 万台电脑被回收，且大部分旧的电脑被出口到发展中国家(如我国、印度和巴基斯坦)进行拆卸。这些国家缺乏能力、法规或政治意愿来实现合理的环境政策。因为新技术的设计和 ICT 公司的销售技术的快速成功，产品生命周期短暂，这造成对废物处理和随后的环境影响的一个沉重负担。

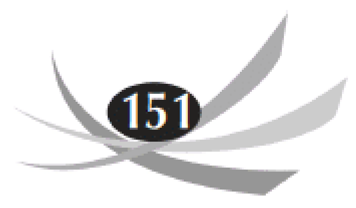
目前，电子垃圾已作为一些伪造部件(特别是电子部件)来源的一部分被记录。未来，控制电子垃圾也许会变得更加困难。首先，使用电子垃圾给伪造者带来的巨大经济利益是不言而喻的。其次，全球范围内，电子垃圾的可用性将继续加强。在 2010 年 2 月，联合国环境署发布的报告中指出：“预测，到 2020 年，在中国和南非，源于电脑的电子垃圾将至多达到 2007 年水平的 400%”。根据 GAO 的研究，适当的回收电子垃圾似乎是不可行的。显然，未来，伪造者将继续有充足的经济利益和电子垃圾组件的来源[AIA2011]。

6.4.4 硬件伪造的影响

在影响硬件供应链安全的众多因素中，硬件伪造的影响尤为显著。据悉，美国反灰色市场联盟(Anti-Gray Market Alliance，AGMA)表示，“甚至有报告称，半导体伪造市场已经占据了世界半导体市场的 5%”。根据该说法，对于 2010 年半导体市场规模约为 2500 亿美元，那么伪造市场的规模约为 125 亿美元。结合 OECD 给出的关于伪造和盗版的经济影响的报告[OECD2008]，可看出硬件伪造不仅仅导致巨大的经济损失，还给其他方面(如社会、文化方面)带来严重的负面影响，危害范围非常广泛。

1. 国家安全

伪造对重要基础设施的潜在影响：在使用时，可造成直接或比预期早的系统故障；获得不安全的系统；削弱加密系统。伪造蔓延到了军事和航空领域。承包商和政府机构所购置的许多元件是用于飞机、坦克车和军舰的电子系统。由于重新设计过于昂贵，所以唯一的选择就是向售后市场购买已经用了数十年的老式且早已过时的元件。这样看来，意



外似乎随时都可能发生。

由美国参议院国防委员会所做的一项调查显示，伪造芯片已经渗透到数种美国国防武器中，包括海军的SH-60B海鹰号(Seahawk)直升机，以及P8-A反潜机。而包括美国半导体产业协会(SIA)在内的产业团体，指出若伪造组件进入国防武器、网络或是医疗设备中，将会变成“定时炸弹”。甚至，有的伪造元件以谍报活动和恐怖主义为目的。某种伪造部件一旦被植入系统中，就会像“特洛伊木马”一样收集特定信息或使系统瘫痪。

2. 对社会经济的影响

(1) 创新和增长。创新一直被认为是经济增长的关键驱动力。在很大程度上，新产品和新工艺的开发和使用刺激了经济增长。创新者通过专利、版权、设计权和商标保护其思想和技术。这种保护是促进创新的关键，同时也是高风险、耗时且昂贵的。然而，伪造破坏创新者的努力，降低了发明者的积极性，因此对研发有极大的不良影响。

(2) 犯罪活动。由于伪造和盗版具有高利润和低风险，因而犯罪网络已开始涉入。假定伪造和盗版将经济收益转给非法货物供应者，至少一部分资金被用来维持进一步的犯罪活动。犯罪集团进行伪造和盗版活动的增长是一个值得关注的经济问题，因为它能以一种腐败和有组织的方式供给犯罪集团进行一系列非法活动的资源，进而破坏社会。

(3) 环境。伪造和盗版可对环境产生负面影响。这一方面是双重的。首先，捕获伪造和盗版产品引起了环境问题，因为破坏这些产品需付出昂贵的代价，带来了相当大的浪费。其次，伪造品破坏环境，例如，电子垃圾拆解过程产生的“三废”不仅直接危害人体健康，而且会对土地、水源造成严重污染。据统计，全球每年产生上千万吨电脑、手机、打印机等电子垃圾，其中70%以上通过各种“灰色”渠道进入我国。与此同时，国内每年产生的电子垃圾如今已达230万吨，仅次于美国的300万吨。但是，目前国内数量庞大的电子垃圾进入循环利用体系的还不足10%。可见，剩余的电子垃圾将对环境产生巨大危害。

(4) 就业。在整个经济层面，伪造和盗版以多种方式影响就业。在经济体中，将出现一种转移，从已认识到的传统雇主转为秘密的操作。在秘密的操作工厂，工作环境较差，就伴有健康和安全风险。而且从事秘密操作的工人的薪酬水平和工资待遇很可能远远低于合法企业保障的工资。

3. 对制造商的影响

除了制造商，以下影响可进一步扩展到其他的硬件供应链参与者，如经销商和零售商。

(1) 销量和价格。因伪造和盗版，公司直接遭受销售额的损失。因欺骗而损失的销售额是很高的，因为几乎每购买一件伪造品意味着合法生产者销售额的降低。在有意或无意购买伪造元件的二级市场上，很难量化销售额损失的影响。

而且，伪造对销售额的中长期影响还附有其他相关问题。首先，伪造和盗版会破坏公司的与时间紧密相关的市场策略。其次，当今的经济理论表明，在某些情况下，随着时间的推移，二级市场上低廉的伪造品的销售可扩大到真品市场上。

就价格而言，因为伪造者没有新产品和新工艺的研发成本，他们能够以较低的价格销售产品从而获取利润。因而，伪造品的出现给制造商及其授权经销商带来了价格压力。例如对于专利，同类产品的非法生产向市场上投放了额外的商品，这将对价格造成下调

压力。

(2) 品牌价值和公司声誉。伪造品可损害公司的品牌价值和生产者的声誉。例如，那些购买真品而事实上买到假货的消费者，当假货没有实现预期的功能时，很可能指责真品的生产商，导致厂商损失了商誉。如果消费者没有发现他们被欺骗，那么他们将不愿购买该生产商的其他产品，且可能与其他潜在买家交流信息，从而给生产商带来了潜在的隐患。此外，受害厂商还会担心因质量不好的传闻而损害品牌形象，或导致与销售商的关系恶化。

(3) 版税。版税是著作权人因允许他人使用其权利而获得的收益。侵权剥夺了权利持有者的利益。而且，版税是由产品的不同元素所支付，这些权利被许可而不是直接购买的。从而，因真品销售额损失，多方将受影响。

(4) 公司投资。强大的知识产权保护提供对新产品和工艺流程的开发投资的激励，伪造严重打击了知识产权，从而公司会降低其投资，不利于研发和其他创造性活动。

(5) 打击伪造和盗版的成本。为打击伪造和盗版，权利持有人开展一系列的活动，如更改产品的设计和使用特殊的包装，对伪造品和其销售渠道进行调查和相关研究，寻求政府的援助、加强公众反伪造意识的活动和对买到伪造品的消费者的相关赔偿，为此他们需要耗费大量的时间和成本。

(6) 经营范围。伪造影响公司的经营规模。公司可能因伪造降低其利润，也有可能损失其品牌价值，从而迫使公司破产或降低公司的经营规模。制造商在缩小经营范围的同时增加了员工失业的风险。

4. 对消费者的影响

伪造元件除了导致目前的财产损失之外，还存在威胁健康和生命安全等危险因素。伪造产品轻则给消费者带来不适，重则危及生命。假如飞机和智能电网等使用了伪造电子部件，则可能发生危及生命的事故，那么人民和国家的安全将造成严重威胁。同时，伪造降低了顾客的满意度，例如，消费者无意购买了带有伪造组件的计算机，该计算机的性能与真机的性能相差太多，从而使消费者对产品极为不满。

5. 对政府的影响

伪造造成 ICT 产品销售量下降和价格降低，进而降低了版权所有者的利润和企业所得税。更低的价格也会导致降低销售税和价值增加税。

除了丧失税收，政府还支付一些有关伪造的其他成本，这些成本包括相关的海关成本和开发和维护法律框架的成本。而且为提高公众对这一问题的意识，政府经常提供资源来发出对抗伪造和盗版的倡议。同时，处理查封的产品也需要耗费巨额开支。

上文曾提及犯罪团伙有时通过对政府官员行贿和敲诈勒索来降低破坏他们的分销渠道和非法活动的惩罚风险。这种行为削弱了公共机构对执法部门和其他政府活动(如监管或认证)的控制。

不可否认，今后半导体和电子部件的仿冒品可能会进入市场有望迅速扩大的智能电网领域。万一系统发生事故，那么引起的后果将不可设想。然而目前，缺乏数据阻碍了量化伪造的影响，也是量化伪造影响面临的主要挑战。而且，尽管硬件伪造的危害深远，但由于伪造品问题不愿被曝光的性质，要把握伪造品危害的整体情况较为困难。

6.5　反硬件伪造

伪造电子元件造成元件供应商和系统公司数百万美元的损失，并占用了大量宝贵的资源，因为需要提供员工解决那些未达到预期目的的元件造成的质量问题。这一影响涉及到电子行业的各个方面，整个电子行业有必要联合起来阻止伪造者。鉴于硬件伪造的种种负面影响，现在各国都在不断开发反硬件伪造措施，以严厉抵制硬件伪造，保护ICT硬件供应链安全。就美国而言，美国半导体产业协会、国家电子经销商协会（NEDA）和政府机构（如国防部）把伪造视为行业的主要威胁。2004年，美国商会创建反伪造联盟来打击对经济、就业和消费者健康和安全构成不断威胁的伪造和盗版。2005年，经济合作与发展组织对伪造的程度和范围进行了评估。2006年6月，美国半导体产业协会成立防伪特遣部队，其致力于教育该行业关于伪造元件和劣质设备的危害，并在其生产和销售中不断抵制伪造品。2007年8月，美国航空航天工业协会举办了"什么是伪造及其解决方案"的伪造峰会。2009年11月，美国商务部技术评价办公室在对伪造电子组件的调查中称，仿冒设备正日益扩散并出现在各个级别的供应链中。2010年，美国审计局（GAO）针对伪造的风险和影响，发布了两份报告：国防供应商报告（国防部应采取持续的行动来开发降低伪造零件风险的计划）和观察工作报告（知识产权——对量化伪造和盗版产品经济影响的努力的观察）。2012年，美国国防授权法案（National Defense Authorization Act for FY 2012，FY12 NDAA）中，指示国防部应发布相关政策和规程来监管伪造电子元件，并对不遵守其政策规定的部门进行严厉的惩罚[WRLLP2008]。

此外，个体商业部门也针对伪造元件的风险逐渐开发出了大量的反伪造措施，如加强供应商的可见性、检测、报告和处理等。下面主要从反硬件伪造项目、法律、政策、技术、管理五方面来阐述如何加强反硬件伪造。

6.5.1　反硬件伪造项目

1. 政府-工业界数据交换计划

政府-工业界数据交换计划（Government-Industry Data Exchange Program，GIDEP）[GIDEP]是政府和行业参与者之间的合作活动。GIDEP于1958年提出，1970年被后勤委员会采纳。自1991年至今，该计划作为一项联合计划执行，由美国海军牵头，与空军、陆军和国防后勤部共同出资。它致力于通过技术信息共享来减少或消除系统、设施和设备生命周期中的资源消耗或研发成本等，并提高系统的安全性和可靠性。

GIDEP的主要目标是：

（1）减少或避免元件研发中的重复试验，节省开支，加快研发速度。

（2）鉴别出有缺陷的产品和可疑产品，使它们不再进入新设计方案，防止重复出现错误。

（3）利用现成的可维护性或可靠性数据和失效经验数据，提高设备和系统的可靠性。

2. 可信集成电路计划

美国没有一个全面的计划来验证其武器系统中的集成电路没有包含恶意电路。为了

应对这一问题，2007 年，国防高级研究规划局（Defense Advanced Research Projects Agency，DARPA）发起了可信集成电路计划（Trusted Integrated Circuits，TRUST）[DARPA]，旨在开发可确保军事系统中集成电路在不可信环境下设计和制造后的可信性的技术，从而提高无论何处生产的集成电路的可信性。

TRUST 计划将信任那些可测量的技术和测试技术。基于在可测量标准中 IC 的信任度，TRUST 与传统方法差别甚大。在 IC 设计和制造过程中，既没有使用可信度量，也没有使用量化可信的测试方法。该计划追求一种形成于检测概率对误报概率之间的度量方法。它提供一种明确的路径来识别被恶意攻击的 IC。

TRUST 由三个一年计划组成。随着待检查的晶体管数量的增多和允许检查时间的减少，每一阶段的测量将变得更加困难。同时，更需要检测集成电路变化。

3. 可信集成芯片计划

美国政府为改变现状，提出了一项新计划，即可信集成芯片计划（Trusted Integrated Chips，TIC）[IARPA2011]。该计划始于 2012 年 4 月 1 日，止于 2017 年 3 月 31 日。TIC 项目集中于研发制造芯片的新方法，来确保主要由海外制造的芯片的安全和保护知识产权。该计划由情报高级研究计划署运作，研究小组成员可直接向国家情报总监汇报成果。

(1) 项目背景。半导体行业一直在飞速发展。美国学术社区和美国工业基地希望开发出高性能集成电路和系统芯片。根据设计，确保安全地制造组件。TIC 计划希望确保美国可以：在集成电路中尽可能获得高性能，获得近 100%的保证设计是安全的而且没有受恶意电路的威胁，在保护知识产权的同时确保设计、功能和性能安全，结合先进的 CMOS 和其他高价值的芯片，实现安全的系统。

(2) 项目阶段。该计划预计持续 5 年，并分为 3 个阶段。第一阶段为两年的基础期，评估初始的 CMOS 电路设计和制造，然后执行 CMOS 设计改进和初始的系统集成。第二阶段和第三阶段都是 18 个月，每一阶段将包括具体的技术目标，将用于决定是否已经取得了足够的发展来进行后续阶段。第三阶段将以最后一组集成芯片和展示安全可靠的芯片结束。在此简洁描述 3 个阶段的计划和主要目标：

第一阶段(2 年)将集中于分离制造过程的开发。这一阶段的主要任务是设计、建造和测试电路演示车辆来演示分离制造。一项提议的电路演示车辆（CDV）芯片必须由先进的集成芯片（如混合的单电路、光子 CMOS、MEMS-CMOS、电源 CMOS、射频互补金属氧化半导体（RF CMOS）、内存 CMOS 及超导的 CMOS 等）组成。这种分离制造包括在初始技术节点处将前道工序和后道工序铸造过程的集成和最优化。用于铸造厂的普通晶片平台将是 200mm 以促进初始原型开发。第一阶段 12 个月的里程碑将是成功的布局、制造和 130nm 集成芯片的特征。24 个月的里程碑将是成功的布局、制造和 130nm 集成芯片的特征以及最初选定的系统应用芯片的集成。

第二阶段（18 个月），将集中于扩展分离制造技术到中间技术节点（65nm）。这一阶段的主要任务是同第一阶段一样，但是在中间技术节点实现和演示。该阶段用于铸造厂的普通晶片平台将是 300mm。第二阶段的里程碑将是成功的 65nm 集成芯片的布局、制造及其特征，以及与初始选定的系统应用芯片的集成。

第三阶段（18 个月），将集中于扩展分离制造技术到最终技术节点（22nm）。该阶段

的主要任务同一二阶段一样，只是在最终的技术节点实现和演示。该阶段用于铸造厂的普通晶片平台将是300nm。第三阶段的里程碑是成功的22nm集成芯片的布局、制造及其特征，以及与初始选定的系统应用芯片的集成。

对于每一个阶段，参与者应计划使用3次制造来开发和制造CDV，以在目标技术节点演示分离制造技术。且不允许国际武器运输条例(ITAR)限制和分类设计。

(3) 项目描述。TIC计划的技术方法是通过将制造业划分为由离岸铸造厂制造的晶体管层组成的前道工序和由更有保障的美国设施制造的金属组成的后道工序，进而保护电路或系统设计。用此方法，设计的意图不会透露给前道工序的制造者。

6.5.2 反硬件伪造的法律建议

1. 进口条例和采购法规

ICT硬件同其他进口产品一样，须遵守进口条例。尽管在供应链的两端使用潜在的技术解决方案，以阻止在硬件全面启动时插入恶意部件，或将颠覆性或伪造的硬件插入关键网络，但是较少的技术可以在各阶段都有效。IT硬件遇到同海外生产的药品一样的问题；制造商拥有在生产和由药店和分销商单向测试时大大降低篡改药品几率的技术。然而，为了减少大量的假药进入供应链，联邦政府通过食品和药物管理局已经建立加强对进口药品的监管和FDA(Food and Drug Administration，食品和药物管理局)测试和拒绝进口可疑药品的政策。尽管进口条例不能完全阻止所有的劣质产品进入供应链，但是它们提供了一个特定于进口ICT硬件的框架。因此，为ICT硬件提供相似的解决方案，需要开发专门针对ICT产品的进口条例[GISC2008]。

除了进口规定，采购政策也可降低硬件破坏威胁。因为采购法规的复杂性和不断变化，这些政策应该流线型，以促进普遍实施。因而，有必要建立能够适应复杂的全球化市场的新型采购政策和实践措施。如为防止供应链中断，可分享持续性、强制性的供应链产品和维护替代来源。此外，国防部有关IT产品的采购政策应不单考虑价格，还需要考虑安全因素。

2. 设立防伪国际标准

大多数行业解决伪造问题的办法是在元件上贴序列号，或在其他很小无法单独贴标签的产品的包装上贴序列号。例如，航空业使用SAE AS5553来防止伪造设备混进航空器中。在电子行业，序列号通常打印在承载元件的盘或托架上。但是也有某些供应商将此类序列标签用于航空业以外的领域，没有标准，用户难以自动收集数据。虽然围绕伪造电子产品的讨论相当多，但到目前为止，人们还未付出一致努力解决这一问题。

正在采用的各种技术包括条形码、二维矩阵和RFID标记。在使用行业标准后，收效会大于针对伪造者的斗争。可以将库存控制流线化，如果公司发现他们使用了有缺陷的元件时，可以更方便地跟踪到有故障的系统。因此，目前很有必要设立防伪的国际标准。

6.5.3 反硬件伪造的政策建议

1. 经济激励

完全消除源于破坏性和伪造硬件的风险是不可能的。只要动机存在,该行为还会发生。因此,确保采办安全和在关键系统中安装合格的硬件是至关重要的。ICT 公司可提供经济激励措施和扩展可信的铸造项目来控制 ICT 硬件的供应。

市场通常提供足够的激励措施来解决安全问题,然而,这不总适合 ICT 安全的情况。由于市场失灵,提出了许多建议来保证市场有效和应对安全漏洞的创新,但是这些建议都需要政府的有限干预。建议政府提供补贴来指导市场采取更大的安全措施,并降低税收来激励公司从事研发活动。除了降低税收和资本资助,政府还可以与 ICT 公司交流国内研发和制造的各种优势。

2. 保护知识产权

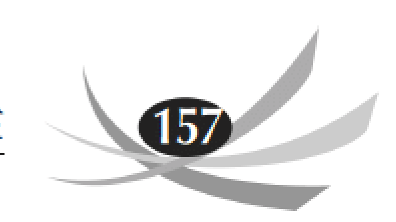
知识产业是国家经济的重要内容,也是企业国际竞争的优势所在,只有保护知识产权,才能确保 ICT 硬件供应链的健康运作。知识产权是任何创新、商业或艺术,或任何商业化使用的独特的名字、符号、标志或设计。知识产权通过给予创作者对作品的创作产权,从而保护他们的经济利益。鉴于保护知识产权的重要性,管理 ICT 供应链中的关键的硬件系统和设施的访问权限将一如既往的重要。

就美国而言,随着政府广泛地展开打击侵犯知识产权(IP)的活动,相对地给伪造者带来更大的压力。2011 年 3 月,奥巴马政府发表了一份白皮书,呼吁国会加强保护 IP 的法律。同年 6 月,ICE 的全国 IP 协调中心执行了连锁反应行动,目标锁定美国国防部和其他美国政府机构的供应链中存在的伪造元件。这项行动横跨了美国八个部门机构,包括 FBI、国防部后勤局以及美国陆军等。而且,奥巴马政府推出国家知识产权执法战略(National IP Enforcement Strategy),加强知识产权的执法力度。奥巴马总统任命的知识产权执法协调员埃斯皮内尔(Victoria Espinel)说,政府计划提高执法透明度和政府协调力度、加强国际合作,确保创新产业供应链的安全。奥巴马政府将知识产权保护的重点放在整条供应链上,因为网络服务商和信用卡公司是版权保护的关键环节。

目前,我国的知识产权法律法规体系建设有序渐进。知识产权行政执法保护和司法保护正逐步加强。国务院统一部署打击侵犯知识产权和制售假冒伪劣商品专项行动,发布《关于进一步做好打击侵犯知识产权和制售假冒伪劣商品工作的意见》,成立国务院打击侵犯知识产权和制售假冒伪劣商品的领导小组,建立健全的知识产权保护长效机制。

3. 行业指导

行业各方合作制定和采用供应链与风险管理标准,制定相关行动方案,与行业竞争公司共同实施,并与政府机构建立公私合作机制。例如,国防部可利用现有的反伪造行动和实践对当前使用的组件和行业建立指导,包括对伪造元件一致、清晰的定义和对伪造元件的预防、检测、报告和处理的一致做法;向国防部和国防承包商宣传这一指导;分析收集的最佳目标的数据和相关资料,并完善降低风险的策略。



6.5.4 反硬件伪造的技术建议

虽然政策提供了一部分必要的策略来阻止关键系统和网络中潜在的硬件伪造和破坏威胁，但是技术发展常常快于政策。除了政策解决方案，还要求自适应技术解决方案来保护硬件避免遭受硬件破坏和伪造。传统的检测技术方法（如X-射线视觉检查）主要依赖于印于产品或包装的显图或隐图，如密封或用图案装饰产品包装、水印等。但这些方法在改进制造和包装技术、识别伪造来源方面有局限性。下面介绍几种较新的技术方法。

1. 认证产品标签

使用认证产品标签（Authenticated Product Labels，APL）和放置于不同等级包装上的标签（放在瓶子内部或瓶盖上、标签识别特定的产品）可突破上述局限性。每一个产品都有大量的已认证的依附于包装内外的标签。不同的标签对应包装的不同单位，例如零售或批发。认证产品标签不仅可检测伪造品，而且还可查明供应链中伪造品的来源。这可有效阻止分销商支持或包庇伪造。而且，在没有与存储中心联系时，认证的产品标签可被远程验证。同时，认证产品标签也可适用于那些使用数字连接且伪造问题特别严重的发展中国家。

客户、分销商和执法部门可使用认证产品标签来检测产品。如图6-3所示，简化的供应链是单个生产者供给多个分销商，每个分销商供应商品给多个零售网点。制造者包装产品后给分销商，分销商将产品给零售网点。认证产品标签依附于在供应链中移动的产品。供应链的每一步都需验证认证的产品标签。分销商验证外部标签在进入供应链的下一步前已正确签署。在遇到匹配错误或丢失标签的情况下，审核员要联系生产商。对于不匹配的标签，因为产品没有有效的签名而被拒绝。生产者存有所有其签署的标签的数据库。该数据库还存有额外的验证信息，如送往的配送中心、传输者和装货日期等。在校验请求时，生产者查看数据库以定位不匹配标签相关的信息。因此，为了识别有关伪造的位置，可在数据库中检索生产时间和运输信息。

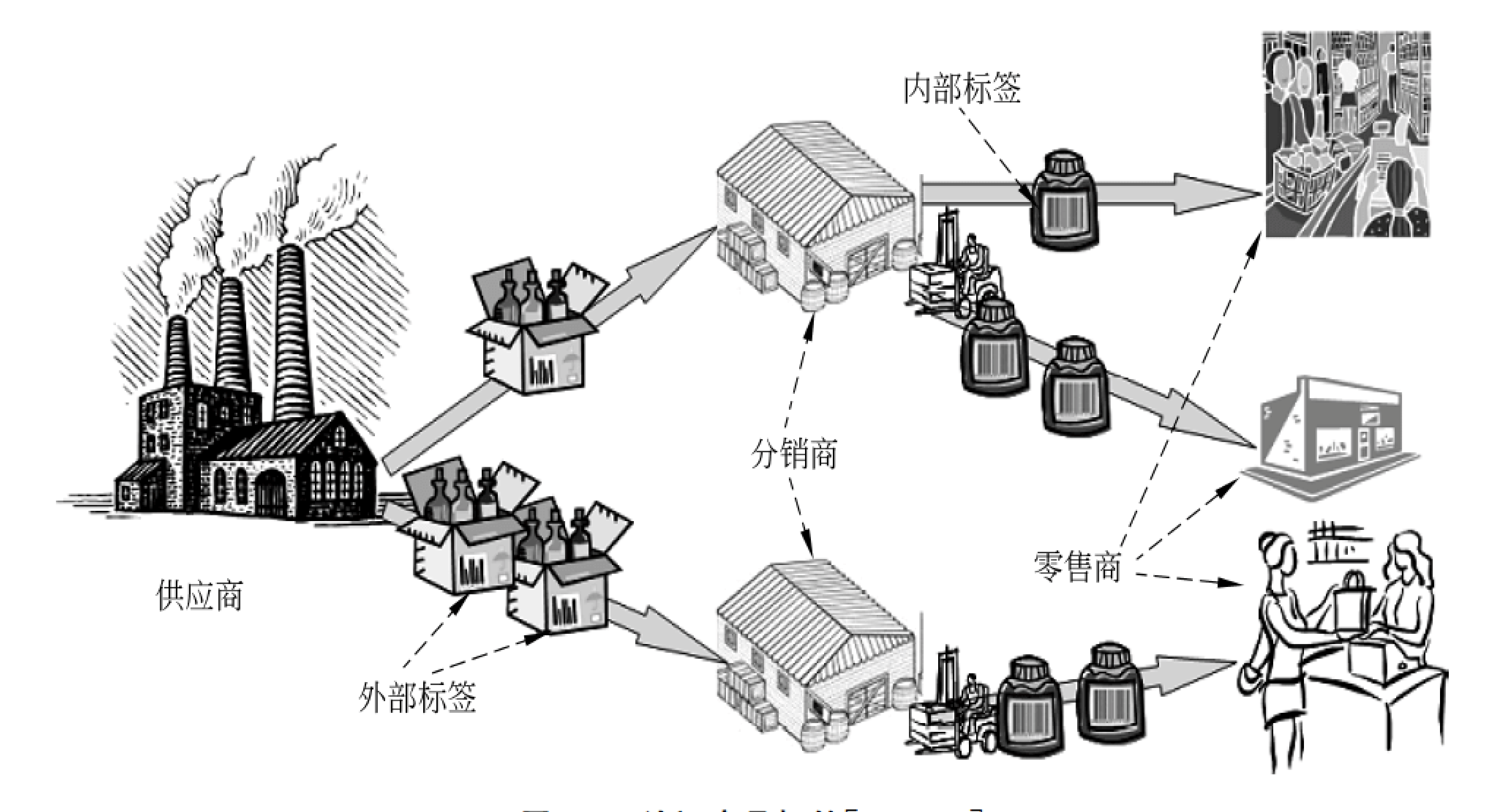


图6-3　认证产品标签[VP2010]

如果内部标签丢失或无效，生产者检索标签数据库以识别造假的分销商。因为外部标签正确签署，生产者查找其数据库以发现其运输信息。因而可识别被复制的分销商的标签。使用简单的搜素数据库过程，生产者即可识别伪造标签来源的分销商[VP2010]。

2. 物理层防克隆功能技术

为确保硬件安全，推荐至少一个预防措施是适当的。在某种意义上，封装（用树脂涂层的电路）是一种预防硬件破坏的对策，因为其不易被破坏。一个更强健的预防方案是运用物理层防克隆功能（Physical Unclonable Functions，PUF）技术设计芯片。物理层防克隆功能是物理的（其基于物理电路的性能）、防克隆的（在有限时间内，其很容易评估芯片，但是攻击者没有无限的时间和资源，不易描述其特征）、功能的（其映射对挑战的反应，意味着以某种方式使用电路（挑战）和接收返回值（反应））。将 PUF 模块集成到芯片中，可使集成电路进行自我诊断，芯片本身将测试其有效性，从而通过 PUF 实现硬件“指纹”，以确保硬件不包含恶意元件。

3. 无线电频率识别和跟踪

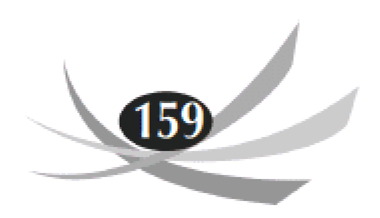
在硬件供应链中，可使用无线电频率识别（RFID）工具。为确保集成电路供应的安全，RFID 提供了潜在的技术方法。据研究机构估计，RFID 技术能使失窃和存货水平降低 25%。设计 RFID 芯片为元件提供可读取和验证的独特标识，该标识通过无线电波发射而不是视距访问项目。RFID 可用于产品信息的快速收集，提高产品的跟踪水平。RFID 可以加强对元件自动识别和管理，集成改进数据采集和全球处理网络，从而带来企业整个流程革命性的改变。在电子组件的特性分析中，产品的跟踪性就是一个影响回收产品的关键因子，在实践中，运用 RFID 电子标签，使产品流和信息流同时为公司提供回收产品的相关现状。

作为当前最有前途的一种产品跟踪技术，RFID 目前已广泛应用于美国国防部、IBM、微软等。RFID 系统基本上由标签、解读器和后端 IT 系统三部分组成，在实际应用中还需要其他硬件和软件的支持。在理论上，其与条形码技术相似，都是使用标签和解读器来读取标签，并依靠标签上交替引用 ID 的 IT 系统，涉及使用一个数据库对象或一类对象。然而，在应用上，RFID 比条形码有一些优越之处，如 RFID 有密钥保护，其数据内容不易被伪造；可同时辨识读取数个 RFID 标签；具有读写能力；可扫描比条形码技术更远的距离。

4. “可信启动硬件”技术

现有的设备遭遇攻击后没有告知功能，例如，伊朗核电站的离心机超速运转，但是发送给监控系统的是正常工作信号。对于这一局面，传统的技术应对策略是加强防护，即通过强化系统安全来避免失密。而“可信启动硬件”技术旨在为硬件添加防篡改措施，保障硬件“不变节”或是让硬件具备失密告知能力，在被侵入、改写后能够被知晓，从而实现可信，让操作人员能够一直在可信赖状态下持续监测目标数据。“可信启动硬件”技术是要让硬件在计算环境中能够被信任。但是如今的硬件对系统安全的支持作用很有限，现有硬件具备的能力也无法被软件充分利用。因此面对网络威胁在复杂环境中丛生的现状，未来的硬件必须具备强大的伸缩性，能够在攻击下保持有效运转。

“可信启动硬件”技术的实现途径比较统一，即在（系统）架构中嵌入防篡改的可信源，



借此让硬件具备辨识能力。目前,能够对此类技术的研发产生助推作用的技术环境诸如:已有专属美国政府的 TCG(测试呼叫发生器)的技术创意,其价值在于使硬件具有遇袭报警的能力,还有 TPM(远程处理监控器)和可信硬件技术,都能改变硬件在失密后不被察觉的被动监控状态;此外,"现场可编程门列技术"的升级也为硬件安全能力提供了技术支持。目前,英特尔公司已经在可信启动硬件技术领域展开大量投入,也证明该技术研发可实现性很强,市场前景广阔。

5. 开发高性能芯片

无论是军用还是民用领域,ICT 硬件供应链的安全对于保证电子产业的有效性来说都极其重要。然而从国家安全的角度看,我们最应关注的是在国防、国家基础设施和情报应用方面的微电子供应。我国需要开发高性能芯片,来提升我国的芯片技术实力。我们可借鉴美国国防部的高性能微芯片供应策略,具体如下:

(1) 为经济发展和低量试产 ASIC,开发商业模式、技术和设备。

(2) 加强对关键半导体生产和设计设备的双边及多边控制。

(3) 加大开发防篡改技术的力度。一旦证明组件具有可靠性,保护芯片免于破坏或逆向工程的反篡改保护就是必不可少的。

(4) 为掩饰 IC 真实功能的开发设计与生产技术。将来可能出现使用不可靠代工的情况。在这种情形下,掩饰提供了一种应对破坏情况的保护方法。现在的 IC 极其复杂,从而在海量逻辑中掩饰设计的真实功能是完全有可能的[DSB2005]。

6.5.5 反硬件伪造的管理建议

目前仅依靠现有的采购和质量控制方法来解决伪造是不行的,还应加强供应商可见性、检测伪造、报告并处理伪造品等。而且,有效解决伪造问题还需要供应商、经销商等在管理方面共同采取措施来降低硬件伪造的风险。

(1) 避免风险的供应来源。避免伪造电子元件的最有效方法是尽可能从原始制造商、分销商或制造商授权的售后供应商处直接购买电子元件。被识别的伪造电子元件大多数是从供应链中不可靠的分销商(未经制造商授权的分销商)处购买的。采购商还应确认供应商们使用预期的伪造品避免政策和措施。这可以通过合同要求和购买订单措辞上实现。采购商可以依法要求一致性认证,测试认证和处理伪造零部件的权利。所有的要求都必须与组织的供应商进行交流,而不是假定供应商们已经采取单边的行动来防止伪造品[HL2010]。

(2) 开发和部署用于在产品的生命周期中从技术和操作层面减少风险的工具和资源,并处理好电子垃圾。目前,已有一些对电子垃圾的处理方案,例如,惠普公司开发了一种回收电子垃圾的模型,该模型强调产品管理,目的是以最低成本有效地管理丢弃的电子垃圾,从而没有对政府施加负担[AIA2011]。还有,巴塞尔行动网络(Basic Action Network,BAN)的电子垃圾管理项目,确保出口到发展中国家的有害电子垃圾被消除。

(3) 逐步由粗放型管理向精细化管理迈进,要探索在对产品采购、使用管理的基础上开展对产品生产、流通的管理和对人的管理。

(4) 存货控制和测试。原始供应商应对硬件进行控制即存货控制和测试。原始组件

厂商应考虑如何处理他们的产品存货，尤其是通过退货和回买过剩的产品；退货政策和零部件的再循环。原始组件生产商冒存货受损的风险接受退货和从顾客手里购买过多的存货。但用户还可通过其他来源来购买伪造元件，然后将这些元件退还给原始组件生产商。

(5) 加强我国的反篡改能力。

① 情报界应开展如下工作：对破坏微电子的关键潜在对手，通过收集、分析与报告等来描述其能力和意图。有了这种新认识后，相关部门应支持技术开发来检测破坏并锁定实施破坏的对手，并确立足以阻止攻击者行为的后续行为。对对手很可能采用的技术有详细的了解，可以将精力集中于敌手很有可能采用的手段，增强篡改检测的有效性。

对于改变微电子组件设计和执行行为的破坏技术，立即开发一份目录，并予以保持。在考虑资金、时间和技术的基础上，确立当前的最佳做法。

② 应开发加强我国反篡改评估能力的投资策略。应严格保护当前和规划的能力；对我国检测能力的深刻了解会让某一敌手根据具体情况制定出攻击性方法，降低他们的成本和操作不确定性。

③ 确定攻击性国家反篡改开发和评估项目。对于某一给定组件，一旦确定了适当的可靠级别，应对该组件使用有效、可制造且承受得起的反篡改技术，确保维持住这种可靠性。

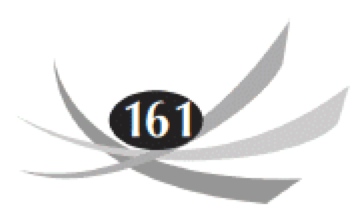
④ 每年发动一次竞争来实施上述的防御方法。该竞争将提供防御技术有效性的评估，并增强风险管理过程中的信心[DSB2005]。

此外，从系统的角度来加强对硬件供应链的管理，从而强化供应链的安全性，从而间接降低硬件伪造的可能性。

① 加强和鼓励科学教育，加强对伪造及其影响的意识，以行业为主导全面落实全球通用标准和推广最佳安全方法和技术，确切地保障 ICT 硬件供应链的安全。并在解决供应链漏洞问题时，采用自下而上和自我调整的方法，使最了解 ICT 供应链流程的各相关方对当前的做法进行评估，并就如何降低风险提出建议。

② 加强对 ICT 硬件供应链安全的战略研究，对我国的 ICT 硬件供应链安全管理政策提供充分的战略研究支持。例如，加强对可编程元件的设计，实现固件完整性和信任评估的设计研究。国防部应该与工业部门和其他政府机关合作，共同资助高校研究，以保证国内有足够的科研人员和精通可编程软件开发和应用的工程师投身到这项工作中来。一个用意明确，在固件完整性方面的国防部项目，极有可能导致对这些可编程组件相关方面的进步的快速发展、宣传和接纳。还可效仿国外，成立开放组可信技术论坛(OTTF)，该论坛是直接针对供应链安全要求 ICT 产业界参与的一项行动。该组织旨在促进采用最佳做法，在产品进入全球供应链的过程中改进其安全性和完整性。论坛不仅制定了一个框架，提出了改进产品开发生命周期各阶段完整性的最有效做法。而且，还制定了一个配套流程以确保生产商根据框架实行最有效的方案。

③ 使用源于全球的零部件来生产我国使用的高技术设备不可避免地会带来风险。我国应加大宣传力度，提高广大用户特别是基础网络和重要信息系统的主管和运营单位的信息安全意识，提高政治觉悟。对于国产产品可以满足使用需求的，要引导其自觉使用国产产品。与此同时，抓紧提高对国外产品和服务的替代能力，鼓励国产产品试点，建设



国产产品试用平台。

参考文献

[AS2008] Adee, S. The Hunt for the Kill Switch, IEEE Spectrum, Volume 45, Issue 5, May 2008: pp 34-39.

[AS2012] Asaf Shabtai, Uri Kanonov, Yuval Elovici, Chanan Glezer and Yael Weiss. Andromaly: a behavioral malware detection framework for android devices. Journal of Intelligent Information Systems, Vol. 38, Issue 1, February 2012: pp 161-190.

[AIA2011] AIA. Counterfeit Parts: Increasing Awareness and Developing Countermeasures. March 2011.

[BH2008] Brian Hughitt. Counterfeit Electronic Parts: Trilateral Safety and Mission Assurance Conference, April 2008. http://www.hq.nasa.gov/office/codeq/trismac/apr08/day2/hughitt_NASA_HQ.pdf.

[CNA] Risk Control Industry Guide Series: Electronic Component and Hardware Manufacturing Industry. http://www.cna.com/vcm_content/CNA/internet/Static%20File%20for%20Download/Risk%20Control/Industry%20Guide%20Series/ElectronicComponenent&HdweMfg.pdf.

[DSB2005] Defense Science Board. Defense Science Board Task Force On High Performance Microchip Supply. February 2005.

[DA2007] Dakshi Agrawal, Selcuk Bakter, Deniz Karakoyunlu, Pankaj Rohatgi, Berk Sunar. Trojan Detection using IC Fingerprinting, 2007 IEEE Symposium on Security and Privacy, 20-23 May 2007: pp 296-310.

[DS2013] David Safford. Integrity Enhancements for Embedded Linux Devices, 2013. http://selinuxproject.org/~jmorris/lss2013_slides/safford_embedded_lss_slides.pdf.

[FI2013] Frank Imeson, Ariq Emtenan, Siddharth Garg, and Mahesh V. Tripunitara. Securing Computer Hardware Using 3D Integrated Circuit (IC) Technology and Split Manufacturing for Obfuscation. Proceedings of the 22nd USENIX Security Symposium, 14-16 August 2013: pp 495-510.

[GAO-11-404] United States Government Accountability Office. Space and Missile Defense Acquisitions: Periodic Assessment Needed to Correct Parts Quality Problems in Major Programs. June 2011.

[GAO-12-361] United States Government Accountability Office. IT Supply Chain National Security-Related Agencies, GAO-12- 361, March 2012.

[GAO-12-375] United States Government Accountability Office. DOD Supply Chain Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms. GAO-12-375, February 2012.

[GISC2008] Global Innovation and Strategy Center. US Reliance on Foreign IT: Mitigating Risks Associated with Foreign Sources of Hardware Components. Summer 2008 Project 08-03, August 2008.

[GTISC2012] Georgia Tech Information Security Center and Georigia Tech Research Institute. Emerging Cyber Threats Report 2013. Georgia Tech Cyber Security Summit 2012, 2012.

[HB1982] Helmut K. Berg, Prakash Rao and Bruce D. Shriver. Firmware quality assurance,

Proceedings of the June 7-10，1982，national computer conference，June 7-10，1982：pp 3-10.

[HL2010] Henry Livingston. Securing the DOD Supply Chain from the Risks of Counterfeit Electronic Components. 2010.

[HT2009] Rajat Subhra Chakraborty，Seetharam Narasimhan and Swarup Bhunia. Hardware Trojan：Threats and Emerging Solutions. 2009 IEEE International High Level Design Validation and Test Workshop，November 4-6，2009：pp 166-171.

[IPPAD2013] The IP. com Prior Art Database. Method to detect a firmware supply chain attack，2013. http://ip. com/IPCOM/000230066＃.

[IARPA2011] Iarpa. Trusted Integrated Chips （TIC） Program，IARPA-BAA-11-09. October 26，2011.

[IS2005] Irene Schipper & Esther de Haan. CSR Issues in the ICT Hardware Manufacturing Sector. SOMO ICT Sector Report，September 2005.

[JIL2003] Joseph I. Lieberman. White Paper：National Security Aspects Of The Global Migration Of The U. S. Semiconductor Industry，June 2003. https://www. fas. org/irp/congress/2003_cr/s060503. html.

[JH2004] James Hendricks and Leendert van Doorn. Secure Bootstrap is Not Enough：Shoring up the Trusted Computing Base. Proceedings of the 11th workshop on ACM SIGOPS European workshop，September 2004：pp 11-es.

[KC2009] K. Chen. Reversing and exploiting an Apple firmware update. Black Hat USA. 2009.

[LL2009] Lang Lin，Markus Kasper，Tim G uneysu，Christof Paar，and Wayne Burleson. Trojan Side-Channels：Lightweight Hardware Trojans through Side-Channel Engineering. Cryptographic Hardware and Embedded Systems-CHES 2009，Volume 5747，2009：pp 382-395.

[LD2010] L. Duflot，Y.-A. Perez. Can you still trust your network card? CanSecWest，2010. http://www. ssi. gouv. fr/en/the-anssi/publications-109/scientific-publications/conference/can-you-still-trust-your-network-card-200. html.

[MT2010] Mohammad Tehranipoor and Farinaz Koushanfar. A Survey of Hardware Trojan Taxonomy and Detection. IEEE Design & Test of Computers，Volume PP，Issue 99，2010.

[MP2009] Miodrag Potkonjak，Ani Nahapetian，Michael Nelson and Tammara Massey. Hardware Trojan Horse Detection Using Gate-Level Characterization. Design Automation Conference，26-31 July 2009：pp 688-693.

[MH2010] Matthew Hicks，Murph Finnicum，Samuel T. King，Milo M. K. Martin，and Jonathan M. Smith. Overcoming an Untrusted Computing Base：Detecting and Removing Malicious Hardware Automatically. 2010 IEEE Symposium on Security and Privacy (SP)，16-19 May 2010：pp 159-172.

[MBS2012] Malek Ben Salem. Security Challenges and Requirements for Industrial Control Systems in the Semiconductor Manufacturing Sector，2012.

[MHS2008] Marcus H. Sachs. Supply Chain Risk Management：Can we Secure the IT Supply Chain in the Age of Globalization? October 2008.

[OECD2008] OECD. The Economic Impact of Counterfeiting and Piracy，2008.

[PWC2011] PWC. Transportation &Logistics 2030 Volume 4：Securing the supply chain，2011. https://www. pwc. com/en_GX/gx/transportation-logistics/pdf/TL2030_vol. 4_web. pdf.

[RS2009] Rajat Subhra Chakraborty，Francis Wolff，Somnath Paul，Christos Papachristou and Swarup Bhunia. MERO：A Statistical Approach for Hardware Trojan Detection. Cryptographic Hardware

and Embedded Systems-CHES 2009，Volume 5747，2009：pp 396-410.

[SS2013] Sherri Sparks. Frontiers in Cyber Security：Beyond the OS，2013 DHS S&T/DoD ASD (R&E) CYBER SECURITY SBIR WORKSHOP，July 23-24，2013.

[SB2013] Scott Borg. ISA Guidelines for Securing the Electronic Supply Chain，2013 Internet Security Alliance，2013.

[SJ2008] Susmit Jha，Sumit Kumar Jha. Randomization Based Probabilistic Approach to Detect Trojan Circuits. 11th IEEE High Assurance Systems Engineering Symposium，3-5 Dec. 2008：pp 117-124.

[USDC2010] U. S. Department Of Commerce，Bureau Of Industry And Security and Office Of Technology Evaluation. Defense Industrial Base Assessment：Counterfeit Electronics，January 2010.

[VP2010] Vivek Pathak. Improving Supply Chain Robustness and Preventing Counterfeiting through Authenticated Product Labels. 2010 IEEE International Conference on Technologies for Homeland Security (HST)，8-10 Nov. 2010：pp 35-41.

[Verisign2013] Verisign. 2013 Cyber Security Disruptors：An Overview. Verisign Public，2013.

[XWHS2008] Xiaoxiao Wang，Hassan Salmani，Mohammad Tehranipoor，and Jim Plusquellic. Hardware Trojan Detection and Isolation Using Curren Integration and Localized Current Analysis. IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems，1-3 Oct. 2008：pp 87-95.

[XWMT2008] Xiaoxiao Wang，Mohammad Tehranipoor，and Jim Plusquellic. Detecting Malicious Inclusions in Secure Hardware：Challenges and Solutions. IEEE International Workshop on Hardware-Oriented Security and Trust，9-9 June 2008：pp 15-19.

[YL2011] Yanlin Li，Jonathan M. McCune，and Adrian Perrig. VIPER：Verifying the Integrity of PERipherals' Firmware. Proceedings of the 18th ACM conference on Computer and Communications Security (CCS'11)，October 17-21，2011. pp 3-16

[YJ2009] Yier Jin，Nathan Kupp，Yiorgos Makris. Experiences in Hardware Trojan Design and Implementation. IEEE International Workshop on Hardware-Oriented Security and Trust，27-27 July 2009：pp 50-57.

[DBW2012] 东北网. 电子巨头索尼报亏年度总计 57 亿美元，2012. http://mobile.dbw.cn/system/2012/05/11/053861188.shtml.

[SINA2008] 新浪网. 华硕苏州厂火灾损失将近 2500 万元. 2008. http://tech.sina.com.cn/it/2008-03-05/01262057428.shtml.

[SINA2001] 新浪网. 爱立信停产手机的起因竟是一场火灾. 2001. http://tech.sina.com.cn/it/t/51693.shtml.

[QYW2011] 企业网. 恶意软件来袭 如何防止服务器变“砖”. 2011. http://www.d1net.com/security/solution/73121.html.

[IHSO 2012] IHS. One Counterfeit Part Every 15 Seconds. May 22，2012. http://www.isuppli.com/Semiconductor-Value-Chain/News/Pages/One-Counterfeit-Part-Every-15-Seconds.aspx.

[WRLLP2008] Wiley Rein LLP. North Carolina Appellate Court Sustains Late Notice Defense. August 18，2008. http://www.wileyrein.com/publications.cfm? sp=articles&newsletter=3&id=8235.

[GIDEP] GIDEP. http://www.gidep.org/.

[DARPA] Darpa. Trusted Integrated Circuits (Trust). http://www.darpa.mil/Our_Work/MTO/Programs/Trusted_Integrated_Circuits_(TRUST).aspx.

[CBP2008] U. S. Customs，Border Protection. CBP，European Union Announce Results of Joint Operation to Combat Pirated Goods. February 22，2008. http://cbp. gov/archived/xp/cgov/newsroom/news_releases/archives/2008_news_releases/feb_2008/02222008. xml. html.

[IHS2012] IHS. Top 5 Most Counterfeited Parts Represent a ＄169 Billion Potential Challenge for Global Semiconductor Market. April 4，2012. http://www. isuppli. com/Semiconductor-Value-Chain/News/Pages/Top-5-Most-Counterfeited-Parts-Represent-a-＄169-Billion-Potential-Challenge-for-Global-Semiconductor-Market. aspx.

第 7 章
ICT 软件供应链安全

7.1 概　　述

在指出硬件供应链安全的同时,我们断然不可忽视软件供应链的安全。因为任何一条供应链绝不会脱离软件的使用,尤其是 ICT 系统。

目前,针对实体供应链的分析已有数十年的历史和经验,而且已经建立了研究和分析框架。而就软件供应链而言,除非拥有一条经验和数据的基线,否则无法建立起这样的框架。软件供应链风险同实体供应链风险有一些相同之处,比如它们都与供应商运营好坏、能否准时交货、能否限制成本以及交付的项目是否符合规格等有关。我们可借鉴实体供应链的分析框架来分析软件供应链的安全。

7.1.1　软件供应链的定义

随着外包的增加和无数风险来源的暴露,安全的 ICT 软件供应链显得愈发重要。人们通常认为供应链是制造和传送硬件或实物的,但也有与软件系统的开发和运营相关的供应链,即软件供应链。目前,据我们调查,对软件供应链的定义有以下几种。

(1)“软件供应链”一词最早出现于 1999 年,英国伦敦大学的 Barbara Farbey 和 Anthony Finkelstein 提出了一种关于开发软件供应链商业结构的研究议程,他们认为软件供应链的架构就是围绕软件供应的关系合同的网络[BF1999]。

(2) 2001 年,英国赫瑞·瓦特大学的 Lynne F. Baxter 和 John E. L. Simmons 提出了一种观点,认为软件供应链不同于供应链,软件供应链仅涉及开发商和用户,并且自动开发商和用户之间存在着一种博弈关系[LF2001]。

(3) 2006 年,新加坡国立大学的 Mabel C. Chou 和 A. Ruchika 认为以软件为中心的供应链指软件在产品中占很大比值的供应链,不但不通过物流传输,而且在产品供应方面,其与传统供应链有很大差别[MC2006]。

(4) 软件供应链由一系列相关联的软件、硬件和服务组成,包括软件维护、发布和部署过程[SJ2006]。

(5) 软件供应链由组件供应商、应用供应商、组装者和用户组成,并以分布式的软件开发方法为基础,其服务管理包括部署、操作、优化等过程[RO2007]。

(6) 2008 年,荷兰半导体公司恩智浦的 Herman Hartmann 和 Tim Trew 认为软件供应链是公司从许多供应商处购买一组组件,后结合自己开发的软件将这些组件集成到产品中的过程。多种行业中都含有软件供应链[HH2008]。

(7) 软件供应链包含物理组件、集成的组件和软件的供应链。例如,商业软件产品供应链包含产品开发组织和供应商;定制软件的供应链包含主采购商、次级采购商、和对定制产品使用的供应链[RJE2010]。

(8) 2011 年,美国卡内基·梅隆大学软件工程研究所(Software Engineering Institute,SEI)将软件供应链定义为开发产品或可更改产品的相关利益者的网络。图 7-1 阐明了软件供应链的概念[CJA2011]。

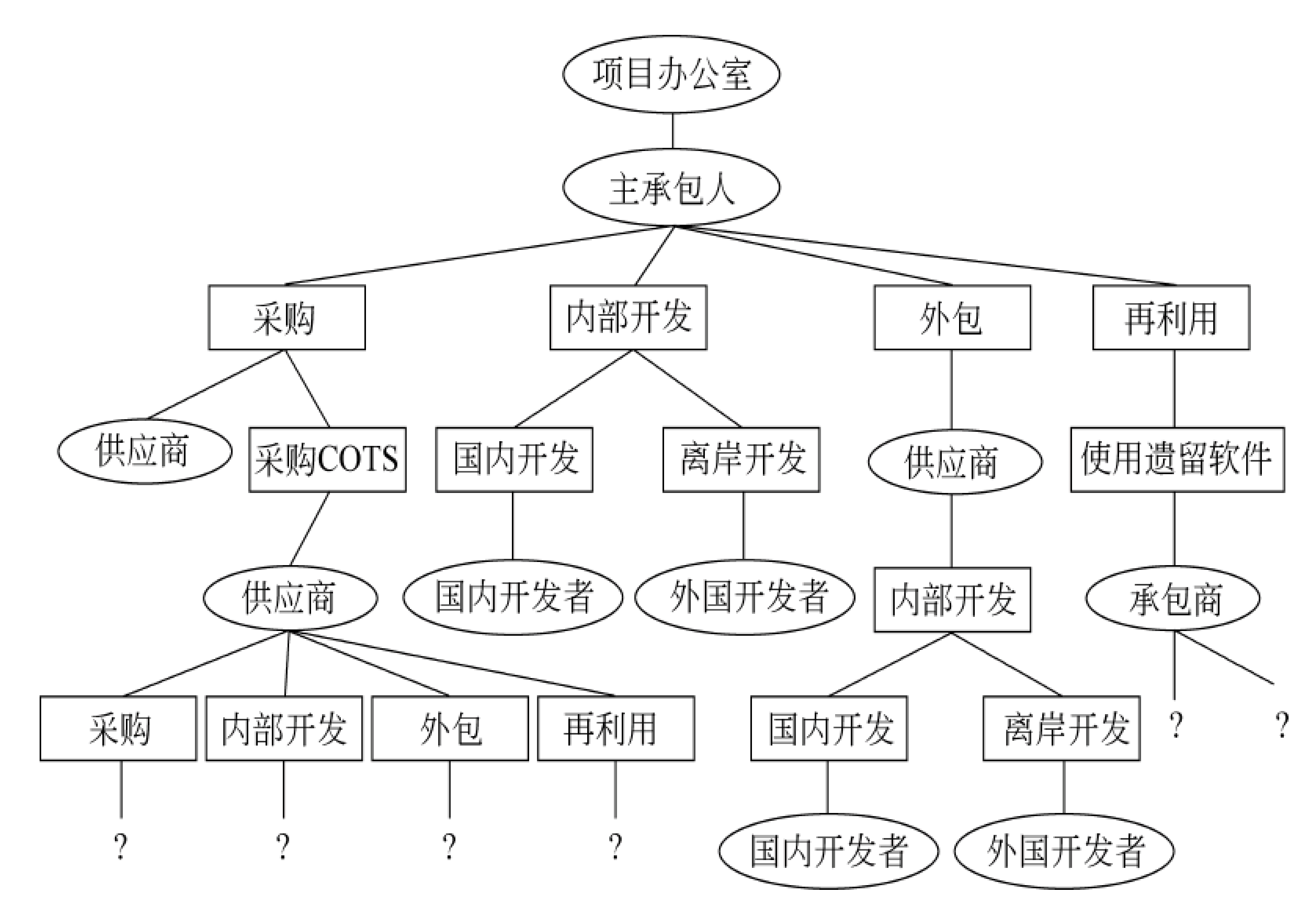


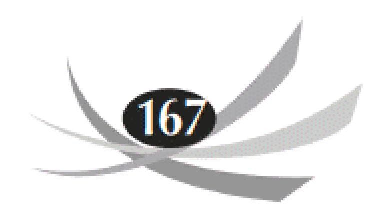
图 7-1 软件供应链[CJA2011]

总之,随着对软件供应链的研究深入化,人们对软件供应链的认识更加完善和成熟化,不再狭义地认为软件供应链是一个纯软件的过程。目前,已获得普遍认可的概念,即软件供应链是从软件采购、开发、测试、交付和维护的整个生命周期过程,其旨在部署软件产品,以达到预期的功能,且产品是可靠的、安全的。软件供应链中的参与者包括政府和行业部门的采购者、信息安全管理者、软件供应商、主承包商、零售商和终端用户[DHS2009]。

与传统供应链相似,软件供应链也具有完整性、有序性、关联性和动态性等特性。但是,软件供应链又区别于传统供应链,例如,软件供应链与硬件供应链在交付阶段的不同。软件产品通常是以一个整体的形式交付,然后在组织内部进行再分配。供应链的完整性问题适用于一次交货。而硬件或集成部件需要多次交付相同的物品,供应链完整性在每一次交货中都得考虑。而且,在多数情况下,硬件规格在交货时就可以被证实是否符合要求,但软件的机能则不可以。当使用软件,遇到开发时没有考虑的情况时,软件组件会表现出我们不期望出现的行为,进而引起安全关注[RJE2010]。

7.1.2 软件供应链的重要性

随着各国不断重视 ICT 安全,如硬件产品及组件(计算机、芯片和软件等)安全,全球的政府部门目前都开始考虑软件供应链对他们的关键系统产生何种威胁,并对此表示担忧。



2011 年 8 月，Netscape 创始人、硅谷著名投资人 Marc Andreessen 在华尔街日报上发表的《软件正在吞噬整个世界》文章称，当今的软件应用无所不在并且正在吞噬整个世界。商业、政府和个体完全依赖软件来执行日常任务。在商业企业、工业控制系统和军事技术领域中，软件应是无错和可靠的。但是，几乎所有的软件都有缺陷。而且，随着外包和商用现成品技术的更广应用，以及开源软件产品的增加，终端用户寻找机会来重新配置或者做一些有限制的增加的方法来安装软件和系统，这些因素都让供应链安全风险变成一个不断增长的忧虑。

近年来，信息技术专业人员不断进行对抗破坏软件的斗争，即对抗各种病毒、木马、蠕虫及各种形式的恶意软件。尽管如此，计算机病毒已变得日益复杂化，其对 ICT 供应链造成的危害也愈发巨大。每天，有数百种我们未知的病毒和木马将潜入 ICT 软件供应链中。假如一种未知的非常强大的病毒能够大量感染 ICT 系统，它可能会导致大规模的系统故障，进而可能关闭整个范围内的自动化流程，甚至使整个 ICT 软件供应链瘫痪。试设想一下，此类病毒感染了依靠 ICT 系统保持业务正常运行的运输和物流供应链，对于其造成的损失，我们将无法估计[PWC2011]。一个简单的例子可以说明问题的严重程度：据有关报告显示，仅 2008 年，计算机病毒在全球造成的经济损失就高达 85 亿美元。2010 年，席卷全球工业界的震网病毒已经感染了全球超过 4.5 万个网络，伊朗遭到的攻击最为严重，60%的个人电脑感染了这种病毒。而且，软件完整性领域的领导者 Coverity 公司 CEO 安东尼・贝特考特(Anthony Bettencourt)曾表示由于软件供应链缺乏有效的管理，全球 2000 多家企业的业绩和声誉都面临着较大的风险。所以，这样的影响将是巨大的。

目前，软件供应链安全已被认为是行业组织进行最佳实践的目标。SAFECode(最佳代码软件保护论坛)组织的执行董事保罗库尔茨说，无论多么安全的开发过程，所有的组件组合在一起，如果你不能做好供应链安全，你将遇到源于恶意参与者或源于独立的弱点的问题。而且，美国国防部负责采办、技术与后勤的副部长办公室乔・哲伯克(Joe Jarzombek)在 2009 年召开的 Web 应用安全计划会议上，其观点代表了美国政府对 IT 供应链安全问题的战略定位：“软件供应链的管理是一个国家安全问题。”总之，软件供应链的安全至关重要，我们万万不可轻视，或忽视之。

7.1.3　软件供应链的复杂性

基于几十年实践收集的数据，对硬件的供应链过程已有广泛的分析。但对软件供应链缺乏同等的实践收集，由此严重限制了对软件供应链的风险分析，同时也无法将用于传统供应链的策略直接用于软件供应链的管理中。软件供应链涉及到一系列问题：谁构建的代码？软件是在何地开发的？设置了怎样的控制流程？软件是如何分发的？是谁集成为最终产品？谁来管理代码？如何进行升级？谁来进行升级？这些问题潜在地引发了软件供应链的复杂性[DSB2007]。

1. 分布复杂性

政府越来越多的依赖于复杂的软件供应链为军事、民用、和情报提供的模块，从而加强了对于软件供应链安全问题的关注。而且，公司或企业加强自身竞争力的策略中也包

括增加国外参与生产的份额。很多公司自身专注于核心技术的开发和研究，而将一些价值少的或者那些他们不具优势的部分外包出去。一些公司十分重视他们对于复杂方案的管理调控能力和整合全球供应链中各个部件的能力，并将这些能力作为他们的竞争优势。所有的这些商务策略都倾向于一个分散的、国际化的生产方式。目前，软件供应链参与者已形成国际化分布。这种复杂性使得采购者理解、监控、采购和管理供应链产品和流程比以往任何时候都困难。

2. 继承复杂性

大多数的软件供应链并不是一个简单的供应商和收购者之间的连接。一个更复杂的 ICT 供应链会涉及内部发展、外包发展、多个商业供应商和遗留系统使用情况的结合。任何时候，复合系统都会继承供应链中的失败风险。采购者和主要供应商已经限制了次级供应商能力的可见性。谁接触到哪些具体的产品或者服务，而对于供应链中的其他人来说是不可见的。通常的情况是，一个收购商，比如美国国防部计划办公室，其仅仅了解与他直接联系的参与者，而对供应链中的次级供应商一无所知。任何一个次级供应商都可以插入缺陷，在以后伺机破坏[RJEJBG2010]。

3. 关系复杂性

软件供应链由多个组织构成，在某些情况下，这些组织之间的关系是正式定义的。例如，一个采购商可同供应商签订一个正式协议，以监管两者之间的关系。通常，采购商提供一系列需求，供应商开发一种满足这些需求的软件产品。正式协议还可用于表明采购商获得供应商的商用现货(COTS)软件的许可，该许可概括了关于采购商使用这款软件产品的任何条款和条件。尽管软件供应链内的许多关系通过正式的协议管理，例如合同或许可证，但是有些关系还是非正式的。例如，通过软件供应链采购和开发的软件产品常需要同现有的操作系统及属于其他供应链的应用程序进行互操作。在实践中，同其他、独立资助的软件供应链的关系往往是非正式的和特别的。

4. 编程复杂性

开发的产品越来越复杂，从而需要编写更多的代码来实现复杂的功能。例如，美国国防部 1980 年推出的宙斯盾系统(Aegis System)需要不到 200 万行代码，2005 年推出的 F-22 战斗机大约需要 400 万行代码，在 2010 年推出的 F-35 战斗机大约需要 1200 万～1400 万行代码，而将在 2015 年实施的未来战斗系统预计需要 1600 万～1800 万行定制代码以及 6000 万行商用现货、政府现货和开源代码。与此相对，1960 年推出的 F-4 战斗机仅有 8%的功能由软件控制，而 F-22 则达到了 80%[DSB2007]。

总之，目前还没有一个管理机构或政策监管供应链中所有的组织，没有一个管理者有权管理所有的组织。管理控制的多个点，这些点导致了一定的编程复杂性，从而很难有效管理。除了管理编程的复杂性，软件供应链的参与者也需要加强对日益复杂的软件产品的了解。

7.1.4 软件供应链的完整性

随着分布性更强的商业软件开发方法的出现，“全球软件供应链中会引入何种产品安全和商业风险”的问题浮出水面。其中颇受关注的一个领域就是软件完整性，例如：当某

一软件产品通过全球软件供应链流动时，一些危险组织可能会有意植入恶意代码，较差的过程控制也可能会无意引入不良代码，这些问题都对软件完整性构成了威胁。在 2010 年，SAFECode 发布的关于软件完整性文章[SAFECode2010]中指出，在软件、组件及服务的外包、开发、测试和分发的过程中，对软件供应链的各个环节实施完整性控制，是目前较为有限的工程方法。软件供应链完整性控制的目的是通过各供应商的安全开发措施（主要是防止产品在供应链流动过程中引入脆弱性）来维持目标产品的基本安全水平。

而且，因为离岸开发、克隆软件、对通过可信机制保持软件打补丁和更新的不断需求，确保软件供应链的完整性是一个比较棘手的问题。在各自的 ICT 系统供应链环节中，为改善被分发的软件的安全保证，所有的软件供应商必须在三个关键的生命周期（软件外包、软件开发和软件分发）中实施有效的软件安全性、完整性和可靠性措施和控制。SAFECode 通过由各软件供应商控制的三个关键生命周期来控制软件完整性，如表 7-1 所示。

表 7-1　软件供应链完整性控制一览表［SAFECode2010］

过　　程	控　　制	
软件外包	供应商合同式完整性控制	• 明确期望 • 所有权和职责 • 脆弱性反馈 • 安全培训
	供应商技术式完整性控制	• 安全传输 • 系统和网络资源共享 • 恶意软件检测 • 安全存储 • 代码交换
软件开发与测试	技术控制	• 人员安全 • 物理安全 • 网络安全 • 代码存储安全 • 编译环境安全
	安全测试控制	• 同行评审 • 安全代码测试
软件分发与维护	发布与分发控制	• 恶意软件扫描 • 代码签名 • 分发 • 传输
	可靠性控制	• 散列密码或数字签名组件 • 通知技术 • 程序运行期间的可靠性验证
	产品使用与维护控制	• 打补丁 • 安全配置 • 自定义代码扩展



1. 供应商外包完整性控制

在外包进程中，供应商提交组件说明、选择组件和服务供应商并接收供应的组件。外包过程中选择和实施软件完整性控制是一个有风险的选择，很大程度上受供应商和他所选择的软件组件供应商之间的关系的影响。供应商之间的关系有三种类型，一是供应商A为供应商B颁发组件供应许可。供应商对其软件（通常是商用现货产品或开源软件组件）颁发许可是其职责所在。确保对产品或组件的安全威胁可在其设计、开发和测试阶段预见和检测；确保外包和生产组件、向客户分发产品过程的安全；供应商向客户提供鉴别产品真伪的方法。二是供应商A雇佣供应商B为其提供软件组件。此时，供应商向经销商分发的软件归经销商所有。供应商使用的软件控制可能是供应商或经销商的，也可能是二者共同拥有的。三是供应商A雇佣供应商B为其提供职员增值服务。经销商和供应商的职员合作开展工程，共享代码库、工作和资源，所有的工程成员都使用相同的软件完整性控制。

在上述的各种关系中，经销商对其供应商所运用的完整性措施和控制实行不同级别的控制。控制级别的区分有助于选择必要的软件完整性控制措施并控制，从而最小化软件供应链完整性的风险。

2. 经销商软件开发完整性控制

软件开发和测试过程中，软件经销商建立、评估、组织并测试软件组件，最终完成并分发软件。软件经销商有丰富的经验来执行有力的管理以及政策和技术控制，从而实现良好的工程实践和知识产权保护。在软件经销商组织内，额外的软件完整性控制存在于其他IT功能中，例如备份和恢复、商业连续性、物理和网络安全以及配置管理系统。

3. 供应商软件分发完整性控制

软件分发包括新产品分发和维护补丁分发。虽然这一阶段可能是供应商直接控制下的软件供应链的最后一个阶段，但是终端用户认为该阶段往往并非供应链的最后步骤，因为软件供应商并不直接将其产品提供给终端用户组织。很多情况下，软件供应商的产品在到达终端客户之前被提交给系统集成者、经销商和授权服务提供者。因此，随着软件组件离开供应商，软件的完整性和可靠性成为供应商和客户的共同责任。

(1) 发行：对产品分发的控制与对软件供应商提供给经销商的代码组件的控制相类似。软件完成后仍需要额外的安全措施，如反恶意软件检测和使客户确保其获取的程序包的完整性的机制。

(2) 软件扫描：应使用最新的恶意软件签名文件和多种商业扫描引擎对产品进行扫描。

(3) 代码签名：软件供应商的产品应用不可更改，但可对需客户验证的特征进行明确的数字标识。

(4) 分发：供应商的在线分发以及通过物理、电子向量分发的方式都应进行保护。客户应可获取代码签名信息和校验信息。

(5) 传递：产品接收者应能证实获取的产品确实来自软件供应商。

事实上，在软件供应链中，完整性保护支持安全性和可靠性。软件供应商通过供应链完整性控制方法，解决外包、开发和分发软件过程中的安全问题，防止任何未经授权而对

软件完整性控制的形式做出的改变,从而保证了安全开发代码的质量,杜绝了因疏忽引入的脆弱性,有效防范了恶意代码植入。然而,验证和分析软件完整性的资源和最好的办法目前还不成熟,这种现实对软件供应商和客户构成了巨大挑战。

7.2　软件供应链风险管理

随着网络技术的发展,软件产品的性质已发生变化,关注的焦点已从独立开发产品到提供技术给较大系统的系统(System of Systems,是指一组为提供特定性能的相互依赖的系统)。作为系统环境的一个例子,软件供应链是多个独立管理的组织通过一系列独立的网络系统提供技术。软件供应链中固有的编程和产品的复杂性往往增加了交付产品中被插入缺陷、漏洞和恶意代码的风险。因此对于建立和维护软件供应链正常运作,有效的软件供应链风险管理是必要的[CJA2011]。

软件供应链风险管理通常指尽力避免软件供应遭到破坏的风险,特别是拖延一个软件组件到达下一个开发商或者用户的破坏;也可指保证供应商没有引入漏洞的软件或组件到产品中。软件供应链中这两种类型的风险是比较常见的。比如,一个软件组件的延期交付可致使依靠这些组件的整个软件系统延期交付,交付一个有漏洞的代码或者用一个较次的软件组件代替,可危及整个载有此部件的系统的行为属性[RJEJBG2010]。软件供应链风险管理贯穿生命周期的所有阶段,始于早期的采购活动,止于系统退役,这是一个长期的过程。在这一过程中,软件供应链管理者需遵循全程控制、先预防后补救的原则,避免遭受风险引起的连锁反应。

为保证软件供应链风险管理得当,在开发软件供应链风险评估时,参与者必须采取一种综合性的生命周期方法,首先分析软件供应链的风险因素有哪些。

7.2.1　软件供应链的风险识别

软件供应链可影响已交付的系统的所有方面。准时交货和成本通常是人们最注意的,但最严重的风险与系统保证有关。软件行为通常是与安全相关联的。我们在探讨软件供应链会遭受哪种风险因素时,可用攻击分析法,即借助攻击行为判定与软件供应链安全相关的风险。对于攻击分析,我们可从攻击动机和攻击平面两方面进行分析[RJE2010]、[DR2010]。

1. 攻击动机

软件供应链攻击通常是利用编程人员或设计人员的失误。故意插入恶意代码通常是利用供应链中的一个漏洞。对员工的审查不足可能让一个内部员工对软件进行非法更改,从而制造出一个可被利用的漏洞后门。因管理不当,用于支持开发的计算软件可能被恶意软件感染。在开发过程中,使用受过审查的员工和强大的配置管理措施,可以降低有意插入恶意代码的风险。

检测缺陷问题是十分复杂的,目前并没有完美的解决方法。一旦恶意代码被攻击者植入系统,它几乎不可能被后续的检测发现。商业上,已经有许多的软件工具来测试代码漏洞,并且这些工具近年来不断被提升。当前的工具,在软件安装之前,能找到占后续发

现错误中三分之一的错误，并且误报率约等于正确判定异常率。此外，对手肯定也有相同的工具。因此，恶意代码可以被设计成能通过这些工具检测的形式。

某种程度上，在一个地域分散式的软件供应链上，故意地插入恶意代码十分困难。然而，现在更大的危险是在交付的产品中，编码者无意留下可被利用的设计错误和编码错误。这种可被利用的软件缺陷，十分普遍。2010 年 9 月 22 日，Veracode 公司公布了半年度的《软件安全现状报告》其整体发现是，大多数软件很不安全。在 Veracode 测试时，不管软件的来源，58%的应用软件没有达到应有的安全级别。

攻击通常试图让软件系统进入开发人员预期不到的一种状态。例如，如果系统执行攻击者提供的代码，即使在软件设计中充分考虑一些具体行为，也可被攻击者改变。攻击者可利用软件缺陷改变系统的行为，比如：访问未授权的数据；制造一些场景导致一项系统服务终止(拒绝服务)；执行攻击者的软件。而且，攻击之所以能成功往往是因为软件程序无法适当的验证数据输入。

2. 攻击平面

基于实用性，对软件供应链安全的范围进行分析。攻击 Windows 系统通常利用以下简短的特性，如开放端口、服务运行、总访问控制、动态生成的 Web 页面和疲软的访问控制。

一个攻击面指标是用来比较多个版本或配置一个系统。它不能用于比较不同的系统。攻击平面的因素包括：

- 目标。攻击者所需的数据资源或流程：例如，目标是 Web 浏览器、Web 服务器、防火墙、邮件客户端、数据库服务器等等。
- 推动者。为达到目标，攻击者使用的流程和数据资源，如 Web 服务、邮件客户端、XML、JavaScript 或者 ActiveX 机制。
- 渠道和协议。攻击者为获得对目标的控制，使用的输入和输出。
- 访问权限。限制关于数据项和功能采取的行动。

攻击者寻找系统中以前成功使用的攻击的特点。例如，一个有 SQL 数据库的系统会受 SQL 插入的威胁。攻击者总是寻求具有高攻击可能性的目标。相仿，收购者可以利用一个类似的措施来识别软件产品具有较低的攻击可能性。我们应该集中精力对付可为攻击提供可能的软件特点，即攻击平面。例如，攻击者经常利用效率不高的输入验证，因此接受用户的输入的软件组件是攻击平面的一部分。攻击平面包含的因素有部件(如电子邮件服务)、特点(如运行时间配置的变化)和实现一个功能的技术。

7.2.2 软件供应链的风险因素

无论何时，只要供应链参与者能接触最终的软件代码或系统，那么危及软件供应链安全的风险都是存在的。这些参与者包括编写、加强和改变产品或系统内容的供应商、分销商、运输者和储存设施。如果没有降低这些风险，那么从供应链上每层继承的风险，将提高安全危机的发生率。因而，对软件供应链的风险考虑不能中断或终止。

软件供应链风险是系统中各软件组件风险的总和，进而开发的产品没有按预期运行或没有以可靠、安全的方式运作。风险可来源于供应商和各个供应链的行动，包括：

[CJA2011]。

(1) 采购者行为——采购需求、来源选择、采购任务执行和活动管理等问题；关于采购的相关问题，将在后续章节中详细介绍。

(2) 供应商行为——架构、验证、部署、设计和编码缺陷，妥协于无意引入的可用设计或编码错误。

在此供应商指商业产品供应商、定制开发和集成承包商、软件开发商和这些组织的分包商。供应商负责软件产品的开发、设计、编码、测试或软件的集成。只要供应商编写软件代码，就会产生导致软件缺陷的错误，因此完美的软件是不存在的。在开发中，供应商编写的代码和设计的缺陷结合在一起，进而在产品或者系统被安置时，允许了未授权组织的代码的插入。另外，有些缺陷允许未授权的访问和受到保护的机能的执行直接危及安全。软件供应链风险分析必须考虑到集成后组件的突发行为，考虑在整合过程中，是否会增加额外风险，毕竟没有组件是无风险的。目前，软件产品在操作环境中受到的威胁往往比开发者想象的要多，而组件的集成是否考虑了这种情况。因此，集成承包商是供应链的整体组成部分。在他们的集成中出现的弱点和他们供应链管理能力影响着整条供应链的风险。

供应商有可能使用商业组件来构建软件系统，但是商业组件可能带来相关的风险，因为一个商业软件组件可以在系统中轻易地部署五年或更长时间。而这期间，可能发生以下情形，从而引入风险到软件供应链中。

- 随着软件组件的使用情况，出现了早期评估中没有考虑的情况，进而弱化了软件组件的功能；
- 新的攻击技术不断出现，而且软件组件本身不断暴露出缺陷；
- 系统中使用新的或者增加扩大使用的临界产品。

(3) 产品——与软件产品相关的缺陷和问题。

针对产品如何影响供应链，以商用现货软件(COTS)为例来阐释。通常，当购买COTS时，采购商对软件产品的安全特性的了解是有限的。如果COTS软件包含重大的安全漏洞，则该软件即为高风险组件。在软件供应链中，当COTS作为软件供应链中的一部分时，高风险的COTS软件同其他软件产品和系统相联络，以生产一个集成的依赖软件的系统或系统的系统。因此，软件供应链继承了这一组成的软件产品和系统的风险。

① 混合代码。软件开发可以使用多种商业模式。从广义上来讲，软件可以分为定制化软件，政府现货软件和商用现货软件。事实上，这一问题要复杂得多，在每一种情况下这些软件类型会相互交叉(如免费软件和开源软件)，而一种商业模式下开发的软件也会应用到另外一种模式中。举例来说，很多商用现货软件开发人员和国防部定制代码开发人员也可能嵌入出处无从考证的开源代码或其他开发人员开发的代码。由于定制软件可以定制化开发特性并易于控制，人们便常常将软件安全和可靠性风险归咎于开源代码软件及商用现货软件。但是，事实并非总是如此，快速成为原型的定制软件会很快融入运行环境而变成不可分割的一部分。在目前阶段，几乎所有的ICT环境都是一种“混合代码”[DSB2007]。目前各方均对留有后门的未保护代码部分表示担心，因为这使得带有恶意的个人或政府有可能破坏软件运行。

② 恶意代码。软件产品一般具有潜在的漏洞，如缓冲区溢出、格式化字符串等。在开发中，代码编写和设计的缺陷结合在一起，进而在产品或者系统被安置时，允许了未授权组织的代码的插入。软件代码缺陷会致使产品发布时间延期或召回、影响客户满意度甚至造成资金流失。利用任何一类软件均可对供应链发动攻击，包括定制软件，提供云服务的软件或嵌入硬件设备的软件。对商业软件开发过程的忧虑通常集中在代码的设计和质量。此外，盗版软件虽然因不能满足国家标准进入不了供应链，但却有可能被当作正版贩卖给消费者。

(4) 操作和维护——随着时间的推移，使用和维护部署的产品或服务的变化引起的操作问题。

对于软件系统来说，供应链安全风险管理措施必须考虑到在软件设计、安装，配置和系统操作时，可能带来的安全风险。通常，软件产品提供比用户需要的更多的功能。在许多情况下，未使用的功能和服务在操作时启动了。当未使用的功能启用时，它可能导致安全漏洞，并增加了操作安全的风险。一般来说，所有非必要的功能应不可用，以便在操作时减少潜在的网络攻击。

另外，软件系统安装和使用不正确(不安全的部署配置，如使用缺省口令的部署配置)可能增加安全风险，所以终端的软件系统用户与硬件系统用户相比，有更多的责任来防止未授权的篡改。

① 安装。在安装期间，软件供应链的挑战在于确保当危险的环境、使用情景、要求及元件演化时，经营风险能够不断被评估和减轻以保证经营目标和资产不会处于危险之中。商业软件元件的部署通常需要五年或更长时间。在部署时出现的风险包括：

- 新的进攻技术和软件的弱点可能被发现。
- 增加功能或变更设计的产品升级会使最初风险评估的结果作废，并可以引入新的漏洞。
- 企业合并、新的次级承包商的出现，或公司的政策、员工培训、软件开发过程的变更可能会取消预期的软件供应链风险管理的实践。
- 随着新产品用途出现，产品的重要性可能增加[RJE2010]。

② 维护。可靠性工程师很早就认识到通过频繁打补丁的方式修复软件可能会引入新的缺陷，从而降低软件的可靠性，虽然一些补丁确实可以实现升级并修复发现的可靠性问题。虽然不是那么明显但一个更为严重的问题是通过补丁蓄意引入新的可利用漏洞或保持旧的漏洞。供应链的整体安全性取决于其最弱的环节，然而，持续不断的修复是供应链不争的事实。很少有供应链可以一气呵成，因此，持续不断的修复给有着各种名目的新参与者提供了机会。

(5) 供应链物流——在供应链的每一阶段对产品或服务不适当的访问控制(例如供应链组件交付或配置控制的故障)；在交付过程中，第三方恶意篡改软件组件。

互联网的高速发展促使软件所处的环境越来越复杂，而复杂的供应链环境不可避免地给软件供应链带来了风险，如未授权的组织可以更改产品或者系统，进而影响其安全属性的风险。如下供应链环境，可给软件供应链带来如下风险[RJEJBG2010]。

① 较低的安全要求，导致所有使用步骤中对于安全的考虑变得无效。

② 当产品或者系统在组织之间转移时，由于对访问的控制不当(物流上的失败)，允许了未授权组织的代码插入。

③ 在使用预留产品或者系统时，作业流程的更改带来了安全风险，或者配置的改变带来了安全隐患(配置控制和补丁管理)。

④ 在弃置产品或者系统时错误地处理信息，给现在操作和未来产品和系统的安全带来危机。

⑤ 扩大的网络连接性和增加的兼容性和系统之间的依赖性增加了系统遇到不利情况的机会。例如，一个为制造商或零售商准时制生产的存储系统和供应商系统有交互的界面。一个大型供应商的系统和买方，制造方，产品运输方都有交互。零售商，制造商和供应商所承担的风险在一定程度上也相交互。在银行诈骗案中，银行就要承担这种风险。要能辨识欺诈行为就要在设计假定时就考虑到其他环节可能已受威胁。在银行诈骗案中，如此的设计假定会导致设计师采用把一个独立的通信信道来确认状况而不用可能已被感染的通信信道提交交易的设计方案[RJE2010]。

⑥ 在软件供应链上的参与是全球的，谁接触到了哪些具体的产品或者服务的对于供应链里的其他人来说是不可见的。通常的情况是，一个收购商，比如国防部(DoD)计划办公室仅仅知道与他直接地联系到的参与者，而对于在供应链中，那些次级供应商没有一点了解。任何一个次级供应商都可以插入缺陷，在以后伺机破坏。

⑦ 国外敌对势力对商用供应链流程的侵蚀。商用开发流程不会也不能保证供应链的纯洁性(未被侵蚀)。软件开发供应链的整体不透明以及软件本身的复杂性使侵蚀难以发现。此外，虽然很多企业会考虑代码的出处以避免知识产权纠纷，从而会使国防部连带收益，但是他们并没有积极寻找恶意植入的可疑代码。

⑧ 软件的采购已经从交付独立的软件发展到提供整合到更大的系统之系统的情境中的能力。这个整合扩大了软件供应链的安全风险。比如，在国防部中，全球信息网络将该组织中的所有系统和软件连接到一起。这样做使得网络中的其他成员都可以在全球信息网络产品或者服务中插入软件安全缺陷[RJEJBG2010]。

软件供应链的风险因素不止上述这些，还包括许多外界因素，如地震、海啸、金融危机等等。外界因素多数是不可控因素，在此不作讨论。

7.2.3　软件供应链的风险评估

风险评估是风险管理的一个基本方面，软件供应链风险评估是从风险管理角度，运用科学的方法和手段，系统地分析软件供应链所面临的威胁及其存在的脆弱性，评估风险事件一旦发生可能给整条供应链带来的影响或人们可能受到的损失程度，提出有针对性的抵御威胁的防护对策和更改措施。针对软件供应链的风险评估并不多，在此，主要简述 SEI 的风险评估方法。

SEI 开发一种风险评估方法来评价软件供应链风险因子和建立软件供应链风险轮廓。软件供应链风险评估以能影响最终结果的关键的风险因子为基础。SEI 的经验表明：需要大约 15～25 个风险因子来建立系统风险的综合概要，每个风险因子都被表示为一个是否问题，是表示风险因子处于成功状态(即对软件供应链的活动带来微小的风险)，

否表示风险因子处于故障状态(即对软件供应链的活动带来严重的风险)。一组标准的软件供应链风险因子：软件供应链目标、计划、合同、过程、任务执行、协调、接口、信息管理、技术、设施和设备、环境条件、合规、事件管理、需求、架构、设计和代码及测试、系统功能、系统集成、运营支持、采用障碍、操作准备、系统风险容忍度、认证许可和维护。这24种风险因子提供软件供应链风险的概要文件。风险因子符合软件供应链风险的来源(采购者行为、供应商行为、供应链物流、产品、操作和维护)。

对于软件供应链风险评估过程，图7-2说明了SEI采用基于风险驱动方法来评价系统化的软件供应链风险的原型。软件供应链风险评估主要包括两部分：识别软件供应链风险因子和分析软件供应链风险因子。

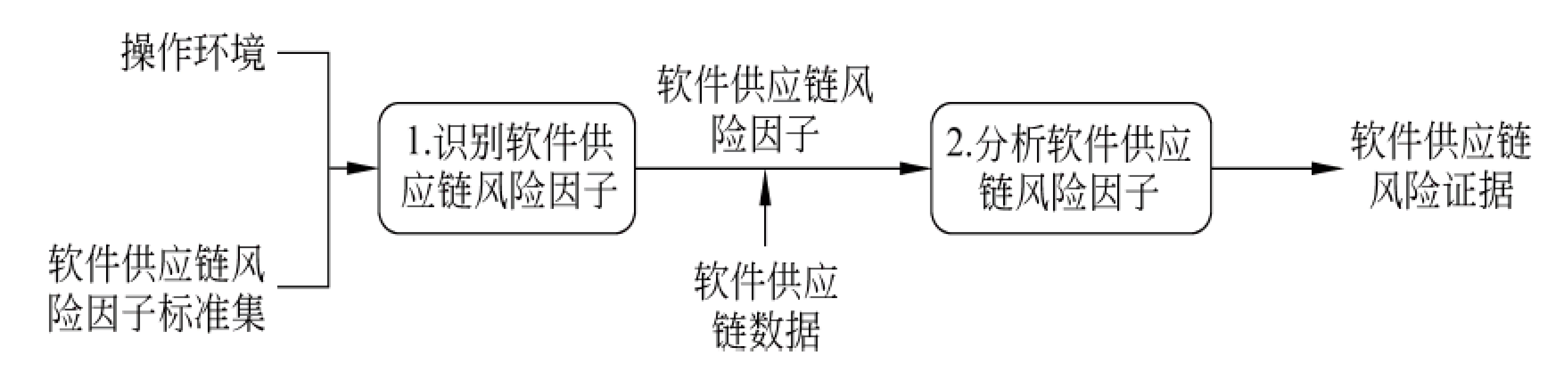


图7-2 软件供应链风险评估[CJA2011]

1. 识别软件供应链风险因子

第一个评估活动(即识别软件供应链的风险因子)的目标是，建立软件供应链的一组风险因子。利用软件供应链风险因子的标准集和操作环境识别一组风险因子。

软件供应链风险因子的标准集是收集供应链任务成功所需的关键因子。为确保标准集在给定的软件供应链中是有用的，风险因子标准集必须适应供应链的需求。操作环境包含任务数据、目标、需求和与特定软件供应链相关的环境。操作环境用于调整风险因子标准集，以满足特定软件供应链的需求。这种调整产生了适应于给定的软件供应链的风险因子组。在第二个活动时分析这组特定的风险因子。

2. 分析软件供应链风险因子

第二个评估活动(分析软件供应链的风险因子)的目标是，评价风险因子如何影响软件供应链的核心任务。当分析软件供应链风险因子时，需要两组输入：软件供应链风险因子和软件供应链数据。

通过第一个评估活动生成软件供应链风险因子。然后通过采访了解该供应链的人员和重审与供应链相关的文档获取软件供应链数据。然后分析每种风险因子产生的风险，并记录分析。例如，分析设计、代码和测试时需要检查设计评审、源代码审查和分析常见的弱点的结果，以及同其他来源的证据[CJA2011]。

7.24 软件供应链的风险处理

目前，软件供应商的开发方法各有不同，但是在软件安全开发处于领导地位的开发者们认为，安全的软件开发方法必须以威胁和风险分析为依据。威胁是指某些个人或组织有动机地攻击系统，而风险是系统受感染后产生的影响和攻击者利用这个软件的可能性的结合。由于软件供应链具有全球性，所以软件供应链不可能不存在风险。对于软件供应链风险，我们可以采取风险规避、风险预防、风险分担、风险分散等处理方法。



1. 风险规避

风险规避是一种风险应对的方法，一般通过采取放弃、中止开发或改变开发方案来避开风险源，消除风险隐患的风险管理措施。规避风险并不是完全消除风险，而是尽可能规避风险给我们造成的损失。风险规避一般适应以下情形：当软件供应链环节中某活动遇到不可控的风险因素时，我们可先处理小风险领域，避免与大风险领域碰撞，等具有抗大风险的能力后，再进入较大的风险领域，从而逐步避免风险损失。因此，规避风险应以合适的方式适时地采取措施。一是减低风险发生的几率，主要采取事先控制措施，如加强软件代码监管；二是降低风险造成的损失，主要采取事先控制和事后补救两方面。

值得一提的一种风险规避方式是风险自留，风险自留是从风险管理全局考虑做出局部牺牲，可以是有意识的，也可以是无意识的。软件供应链常因无法回避某项风险，或完全规避风险是完全不利的，所以采取有计划的风险自留不失为一种规避风险的方式。有计划风险自留是指通过各种计划安排以确保损失出现后能及时获取解决方式以补偿损失。

2. 风险转移

风险转移是供应商在开发过程中，有意识地将自己不能或不愿意承担的风险转嫁给其他企业承担所采取的措施。风险转移并未降低整条软件供应链的风险，只是降低了某环节供应商的风险损失。在软件供应链中，风险转移可分为非保险型和保险型两种。非保险型是通过招标、外包等方式来转移风险。保险型是通过将已识别的供应链风险予以承保，一旦风险发生，由保险人承担相应的风险损失，对于发生概率低而后果可能非常严重的风险，选择保险型是最佳的风险防范方法。

3. 风险减轻

风险减轻是把风险事件的后果和可能性控制在一个可以接受的范围。通常，在项目中，越早采取风险减轻策略及措施，收到的效果越好。例如，在软件开发过程中，开发人员的突然离职等流失问题对软件项目的影响非常严重，我们可以通过重视运用工作团队，建立工作分担机制；核心岗位应建立双角色制度；建立团队分享文化，提倡团队代码共享；加强多岗位人才的培养和储备等方法来减轻人员流失带来的影响。

4. 风险预防

风险预防是一种重要的风险控制方法，其贯穿于软件供应链的整个生命周期中。首先，风险预防为使软件供应链企业管理风险，需建立一个完善的风险管理系统，包括明确管理层的职责、定义软件供应链的风险来源、建立有效的风险监控系统及进行一系列有效的内部控制。其次，需建立一个全面的风险预警系统，以使软件供应链处于安全有序的状态，例如使用软件确保检查列表分析被测软件中的每一个活动。最后软件供应链各环节供应商之间的紧密合作关系，是软件供应链安全运作和风险预防的先决条件。此外，组织需采取综合性的软件确保方法，即组织必须：

- 管理和执行以风险驱动的、强健的、全面的软件开发生命周期。
- 在整个软件生命周期中增加安全"关口"。
- 确保整个组织具有安全意识(如采购人员、开发人员、管理人员、测试人员等)。
- 执行必要的尽职调查，已达到所需的确保水平。

5. 风险共享

风险共享是软件供应链中各企业共同承担供应链风险，从而降低个体供应商独自承担的风险。软件供应链要实现预期的战略目标，客观上要求各节点企业进行合作，实现风险共担、利益共享的双赢局面。例如按风险处理能力分配风险，基于软件供应链中各环节企业的风险承担能力不同，应使它们共享的生产经营风险不超过其承担能力，从而保持相对稳定的合作关系。

6. 风险接受

准备应对风险事件，包括积极的开发应急计划，或者消极的接受风险的后果。对于不可预见的风险，例如不可抗力；或者在风险规避，风险转移或者风险减轻等方法不可行，或者上述活动执行成本超过接受风险的情况下采用。

由于风险因素不断变化，我们对软件供应链风险认识的阶段性和管理技术处于不断完善之中，因此，我们需要对风险识别、风险评估、风险处理及评价方法进行定期检查和完善，以保证风险管理方法适用于现实情况。软件供应链风险管理需定期重复上述各个风险管理环节，从而将整个风险管理过程完全融入到供应链管理中。

但是，人们对风险识别、风险管理技术等具有局限性。而且因为风险太多、有限的供应链能见度、产品保证的不确定性以及威胁，产品机能的不断演化等因素，总预防是不可行的，从而我们应实时关注软件供应链的状态，并不断监管风险（包括信息系统或 ICT 供应链环境的变化）和评价风险管理的效果，对总结的经验教训进行分析并反馈到软件供应链的各环节中，从而不断深化和完善软件供应链风险管理。

7.3 软件供应链确保

软件供应链风险管理的目的就是处理风险，以确保软件供应链的安全。软件供应链确保是确保软件达到合理的可信度，即软件产品能实现预期功能、并且是安全可靠的、防危的。软件供应链确保，在某种意义上，可称为软件确保。软件确保关注于安全的软件组件、软件开发生命周期的安全性、服务中的软件安全以及软件供应链风险管理。

7.3.1 软件供应链确保的定义

软件确保可视为一个保障国家安全和国土安全的关键元素，因为随着互联网应用范围的拓宽，软件日益越来越成为现代化产品和服务的核心构件，是国家关键基础设施建设和应用的重要依赖，如图 7-3 所示。但鉴于软件具有脆弱性和运行时功能的非预期性，这种高度依赖性给关键基础设施带来了巨大的风险，使国防安全和国家经济变得十分脆弱，一旦软件运行异常或瘫痪，那将危及整个社会，造成难以想象的影响。为确保关键基础设施中系统正常运行，软件必须是安全可靠的。

首席信息官执行理事会民意调查发现了软件的两大最重要属性，即“达到承诺功能的可靠软件”和“免于安全漏洞和恶意代码的软件”。软件供应链确保的主要目的是确保开发和维护的软件流程、过程和产品符合管理这些流程、过程和产品的条件和标准。其任务即把软件相关的风险降到最低甚至消除风险。



图 7-3 安全软件应用的需要[JJ2006]

据调查，早在 1978 年软件质量保障会议上，Marilyn S. Fujii 提出了软件确保[MSF1978]的概念，即所有用于提高软件质量的方法，从广义上讲，软件确保方法是用于提高软件质量的任何实践、技术和工具。当时的软件确保实质上仅限于质量确保，但在相当长的时间内，人们普遍认可该观点。在世纪之交，软件确保开始被用来表示软件的可确保的安全性(类似于用信息确保来表示信息的可确保的安全性)。目前，软件确保受到许多联邦机构和实验室的关注，包括国防部、国家安全局(NSA)、NIST 以及 DHS 等。并且，这些机构从不同的角度，用不同的方式对软件确保进行了定义[FLL2009]。

(1) 美国国家航空航天局(NASA)对软件确保的定义。NASA 是世界上较早从事软件确保研究的机构。早在 1989 年 9 月就发布了软件确保指导书[NASA1989]，对软件确保的概念、目的和整个过程进行了详细的描述。NASA 软件确保是一项总的风险识别和安全减轻战略，目的是确保软件产品是高质量和运行安全的。1992 年 11 月，NASA 发布了软件确保标准[NASA1992]，详细阐述了软件确保活动及其研究内容。标准中给出的软件确保定义为通过有计划的系统的活动来确保软件过程和软件产品是符合需求、标准和程序的。程序包括软件开发生命周期过程中的所有活动；产品包括软件、相关数据、文档以及所有相关记录。有计划的系统的活动指需求规范、测试、验证和报告。把这些活动应用于软件开发生命周期就称为软件确保。NASA 的定义强调不但确保软件自身，而且要确保软件开发、运行和维护的过程。为了达到可确保性，软件及开发、运行、维护过程都必须符合需求、标准和程序。

在 2004 年 7 月，NASA 发布了软件确保新标准[NASA2004]，对软件确保进行了更为详细的阐述。新标准将软件确保定义为有计划的系统的一整套活动，目的是确保软件生命周期过程和产品符合要求、标准和程序。

(2) 国家安全系统委员会(CNSS)对软件确保的定义。CNSS 定义软件确保作为可信的级别，即在软件开发生命周期中，无论漏洞是有意设计的，还是意外插入的，软件无漏

洞和软件以预期的功能运行的级别[CNSS2006]。可见,该定义方式类似于信息确保的定义方式。它描述了为确保软件无漏洞和以预期的方式运行,软件本身必须是什么样的,但未说明如何使软件是可确保的。

(3) 美国国防部(DoD)对软件确保的定义。DoD 将软件确保定义为,无论是否有意将漏洞作为软件的一部分设计和插入,软件皆能达到预期功能和无漏洞时的确信程度[MKKB2005]。与 CNSS 的定义相比,该定义更加简洁。

(4) 美国国土安全部(DHS)对软件确保的定义。与 CNSS 的定义相似,DHS 对软件确保的定义[DHS]强调了具有可确保性的软件必须具备的性质:

- 可信性——不存在可被利用的漏洞,不管是恶意的还是有意插入的(与 CNSS 的定义类似)。
- 可符合性——计划的系统的多学科的有效方法可使软件加工和产品符合相应的要求、标准和程序(与 NASA 的定义类似)。
- 可预见性——有理由确信软件在执行时功能是所预期的。

(5) 美国国家标准与技术研究所(NIST)对软件确保的定义。NIST 认为软件确保[NIST]是通过有计划的系统的活动来确保软件过程和软件产品符合需求、标准和程序,以达到:

- 可信性——不存在可被利用的漏洞,不管是恶意的还是无意插入的。
- 可预见性——有理由确信软件在执行时功能是所预期的。

与 NASA 的定义相比,NIST 的定义突出了软件的可信赖性和可预见性。NIST 的定义实质上是融合了 NASA 和 DHS 的定义,说明了有计划的系统的活动和这些活动的预期效果(即取得软件的可信性和可预见性)之间的因果关系。

(6) 软件数据与分析中心(Data and Analysis Center for Software,DACS)和信息保障技术分析中心(IATAC)对软件确保的定义。IATAC 和 DACS 定义软件确保为:软件确保是确信软件可信的基础,它要求软件无论是否出现故障,皆能持续地呈现出所有需要的性质以确保软件在运行中的可信性。从实践上说,这种软件须能抵抗绝大多数攻击;对于不能抵抗的攻击,必须尽可能的容忍;在遭受任何不能容忍的攻击后,能够包容攻击所带来的危害,并尽快恢复到正常状态[DACS2007]。

(7) 最佳代码软件保护论坛(SAFECode)对软件确保的定义。SAFECode 定义软件确保为一种对软件、硬件和服务可免于有意或无意的漏洞和软件达到预期功能的信任[SAFECode2010]。

由此可见,软件确保的多种定义之间是互为补充的,而且就软件可确保的安全性而言,各种定义之间差异甚小。所有定义都涵盖了这一思想,即软件确保必须提供一种合理的确信级别,以确信根据软件需求,软件执行了正确的、可预期的功能。

当前,软件确保已成为安全的核心,是多门学科的交叉,美国 RobertA. Martin 在其报告[RAM2006]中给出了软件确保所涉及的各个学科关系,如图 7-4 所示。

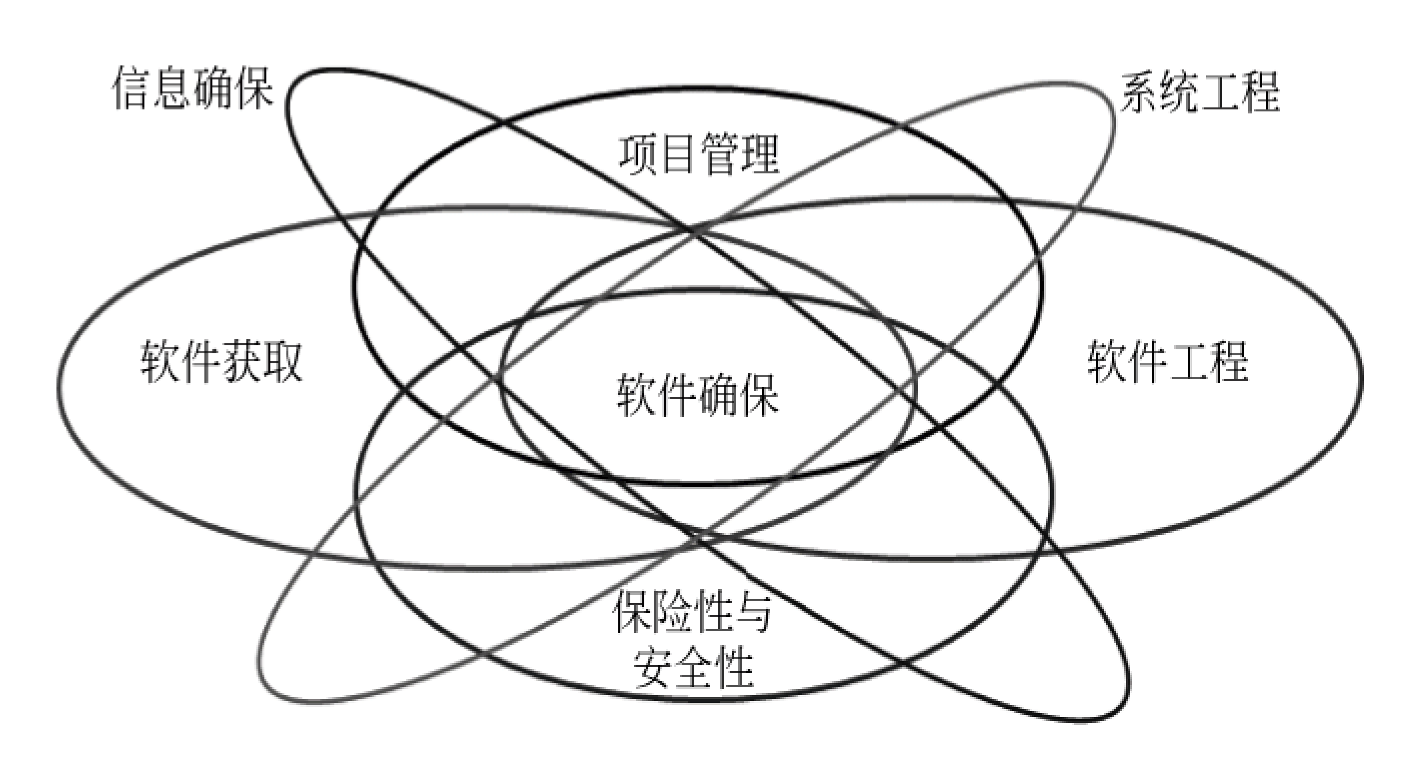


图 7-4 软件确保所涉及的学科[RAM2006]

7.3.2 软件供应链确保的计划

如果无法吓退攻击者又无法检测出恶意软件，那如何确保软件在关键情况下的正常运转？事实上，从来都没有绝对的保障。软件确保实际上不是绝对保障而是智能风险管理。对此，美国国土安全部、国防部和标准化研究院(NIST)都专注于在针对软件开发、采购、供应链管理、教育和培训、工具和测量的方法、产品、标准方面的软件安全相关的进展，并开发了相应的软件确保计划。

1. 美国国土安全部软件确保计划

2003 年 6 月，美国国土安全部成立了网络安全部门(National Cyber Security Division，NCSD)，其主要工作是与私营部门、公共部门和国际实体协作，确保网络空间安全及美国的网络空间资产，并协助实施《确保网络空间安全的国家战略》[DHS2003]。

软件确保是 NCSD 实现其战略目标的一种措施。确切地说，软件确保是 DHS 的一项旨在提高软件完整性、安全性和可靠性的主动战略。DHS 软件确保计划是基于《确保网络空间安全的国家战略》中第 2 至 14 条行动建议的。软件确保计划主要解决软件的可信性、可预见性和可符合性方面的问题。作为国土安全部努力降低风险计划的一部分，软件确保计划努力减少软件脆弱性、最小化漏洞可被利用性，并且努力提出增强可信软件开发过程和产品的方法。所提出的软件确保框架鼓励生产、评估和获取高质量的安全软件。

软件确保计划为软件生命周期(SDLC)中如何解决人员、过程、技术和获取问题提供了框架。该框架鼓励生产、评估和获取高质量的安全软件。处理安全缺陷和漏洞的传统方法是打补丁，该计划寻求从传统方法转变到在整个软件生命周期中对软件产品的开发和应用进行例行检查监督，以确保软件的可信性、高质量和安全性。

国土安全部软件确保计划目前成立了 7 个软件确保工作组，分别对软件确保的相关问题进行研究。截至目前，国土安全部已发布了一些关于软件确保的指导文档。CBK(Common Body of Knowledge)草案[STR2006]为大学、研究所等科研机构的教师设计安全软件工程课程提供了一个基础。为了对软件开发人员进行培训，国土安全部对 CBK 草案进行了补充，并发布了一份补充文档 EBK(Essential Body of Knowledge)[DHS2007]。为了定性和定量地评估软件所提供的确保程度，DHS 软件确保计划于 2008 年 5 月发布了软件确保度量指导文档[SAF2007]，该文档为定量评估软件确保技术被集成到软件生

命周期过程中的程度，以及从这些过程所生产出来的软件的可信赖性提供了一种方法。为了解决安全软件的获取问题，DHS 软件确保计划于 2007 年 9 月 10 日发布了一份由政府、科研界和业界联合制定的指导文档[MLP2007]，以解决不同部门在软件获取过程中所关注的问题，该文档的目的是就如何在软件获取过程(包括计划、合同、实现、接收和维护等阶段)中融入软件确保提供指导。2007 年 9 月 30 日，DACS 针对软件项目管理发布了报告[EF2007]，旨在收集和展示软件确保是如何影响软件项目管理的，并为量化软件确保对软件开发的影响提供了工具和资源。此外，DHS 软件确保计划还资助了 CWE (Common Weakness Enumeration)、SAMATE(Software Assurance Metrics and Tool Education)等软件确保项目。

2. 美国国防部软件确保计划

DoD 软件确保计划源于 1999 年国防科学委员会(Defense Science Board，DSB)发布的全球化与安全年度报告[DSB1999]。报告建议国防部开发软件确保计划，以增强国防部处理对国外生产的商业软件的依赖所导致的潜在风险，这些建议在 2003 年 7 月得到了回应。同年，国防部首席信息官(Assistant Secretary of Defense (Networks and Information Integration)，ASD/NII)建立了软件确保计划，以便在把商业软件应用于政府环境之前对其风险进行检查。紧随着软件确保计划的成立，ASD/NII 在 2004 年 12 月联合国防部秘书处下属的采办、技术和后勤办公室(Office of the Under Secretary of Defense of Acquisitions，Technology and Logistics，OUSD/AT&L)成立了国防部软件确保老虎队，其致力于研究软件保障问题，并已开发出了通过系统工程、源头选择、设计、生产和测试等方式管理风险的一整套策略。该策略确定风险管理的关键要素在于系统部件和子部件的关键性优先次序，并设置了特别的程序以及投入更多的精力确保对于任务成功与否起着最关键作用的系统部件[DSB2007]。

3. 美国宇航局软件确保计划

NASA 认为软件确保由以下学科构成：软件质量(包括软件质量工程、软件质量确保、软件质量控制)、软件保险性、软件可靠性、软件核查和验证，以及独立软件核查和验证。NASA GSFC 软件确保网站上给出了这 5 门学科的详细介绍。NASA 在其网站上公布了新的软件确保指导，该指导从 10 个方面对软件确保进行了非常详细的阐述。由 NASA 资助的 NASA RSSR(Reducing Software Security Risk)计划旨在定义一套形式化分析方法，以便把安全性融入到现存的或正在形成的研发高质量软件和系统的实践中。

NASA 软件确保中心、NRL(Naval Research Laboratory)、NIST、OMG 等机构也在积极从事软件确保的研究。特别是为了促进软件确保的研究，OMG 成立了软件确保特别兴趣组(OMG SWA SIG)，任务是建立软件可信赖性信息分析和交换通用框架。SWA SIG 的一项值得提及的项目是软件确保生态系统(Software Assurance Ecosystem)，它是软件确保需求、论证和证据等相关信息交换的通用框架，它把来自于不同软件工程领域(如逆向工程、静态分析等)的工具和成果进行了整合[FLL2009]。

7.3.3 软件供应链确保的三要素

在保证代码通过可重复的安全软件开发实践的应用变得更加安全的情况下，讨论最

频繁的就是软件确保。然而，当不断的增加和恰当的关注于通过安全的开发方法消除软件脆弱性，这代表软件确保的另一个方面。客户和软件供应商的一项重要考虑是用于处理软件组件在采购、开发和分销过程的安全，因为各种潜在的攻击对象存于整个软件生命周期中。

实际上，软件确保包括一种供应商、服务或解决方案提供商、客户的共同责任，包括如图7-5所示的三个方面：安全性、完整性和可靠性[SAFECode2010]。

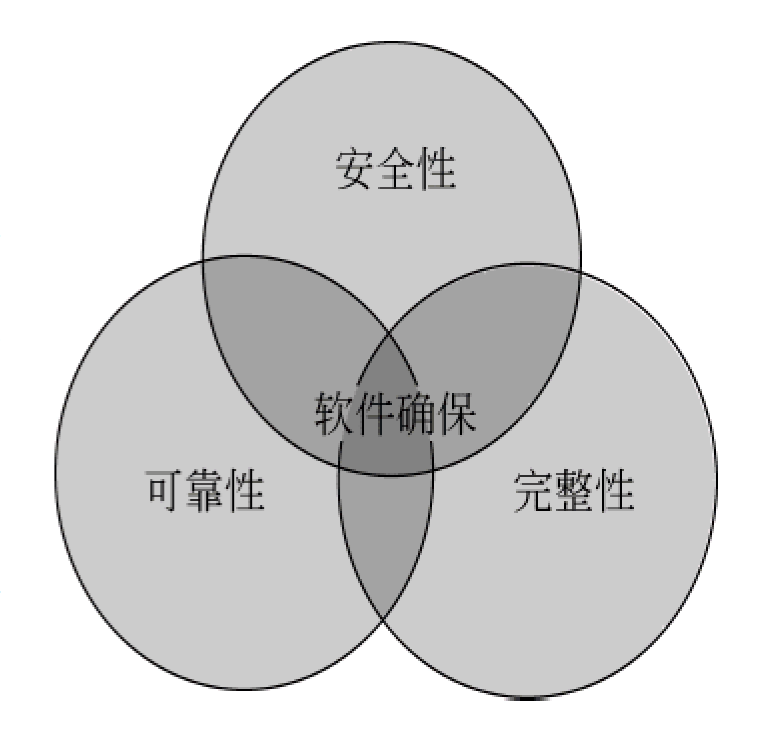


图7-5　软件保障性三要素[SAFECode2010]

(1) 安全性。安全性是指软件在被恶意攻击时，其功能能够正确执行。安全性要求开发人员尽量保证软件在执行过程中只执行预期的操作，避免非预期行为的出现。大量研究表明，在软件开发周期的早期阶段考虑安全性，学习和理解常见威胁、安全的设计方法、风险分析及测试对于软件的安全性至关重要。从而在软件的设计、开发和测试过程中可预见并解决软件安全威胁，就需要把重点放在与安全相关的代码质量特征(如避免缓存溢出)和功能需求(例如护照号码必须在数据库中加密)上。

(2) 完整性。在外包、生产软件组件和向客户分发软件的过程中可解决软件安全威胁。这些过程包括了相关的控制手段，用于进一步确保不存在未经供应商允许而对软件做出的修改。

(3) 可靠性。软件不是仿制品，且供应商为客户提供区分软件真伪的相关方法。IEEE对软件可靠性的定义为：在特定条件和特定时间内，软件不引起系统失效的概率，称为软件可靠性。该概率是关于系统输入和系统使用的函数，也是软件中存在错误的函数。

7.4　软件供应链安全模型

软件作为软件供应链的核心，其安全的重要性不言而喻。有时，我们不得不花大力气来保护ICT软件供应链的安全，其中包括在软件开发过程中限制软件的访问权限，扫描版本中的恶意代码，以及将数字签名用于产品中的二进制文件，以便用户确定交付的软件是否来自原始的供应商。而且，SAFECode执行官Kurtz说："开发安全软件是一门不断发展的科学"。在该节，我们将介绍为保证软件供应链中开发过程的安全，常采用的几种软件供应链确保模型。

7.4.1　S^3R

S^3R(Security、Safety、Reliability、Survivability)软件确保模型(如图7-6所示)可分为4个维度，即软件确保服务、软件状态、软件确保措施及时间。

2004年，在美国第二届国家软件峰会所确定的国家软件战略中，软件确保被认为当

前需要提供4个方面的核心服务，即生存性、可靠性、保险性和安全性。软件状态是指软件开发生命周期中的各个阶段，即概念设计、需求分析、设计、编码、测试、集成、运行等阶段。软件确保措施包括人员、技术、战略3个方面。根据不同的开发阶段和所关注的服务，采取的措施应不相同。最后，通过时间维来表明软件确保的概念、技术、服务等在不断向前发展。

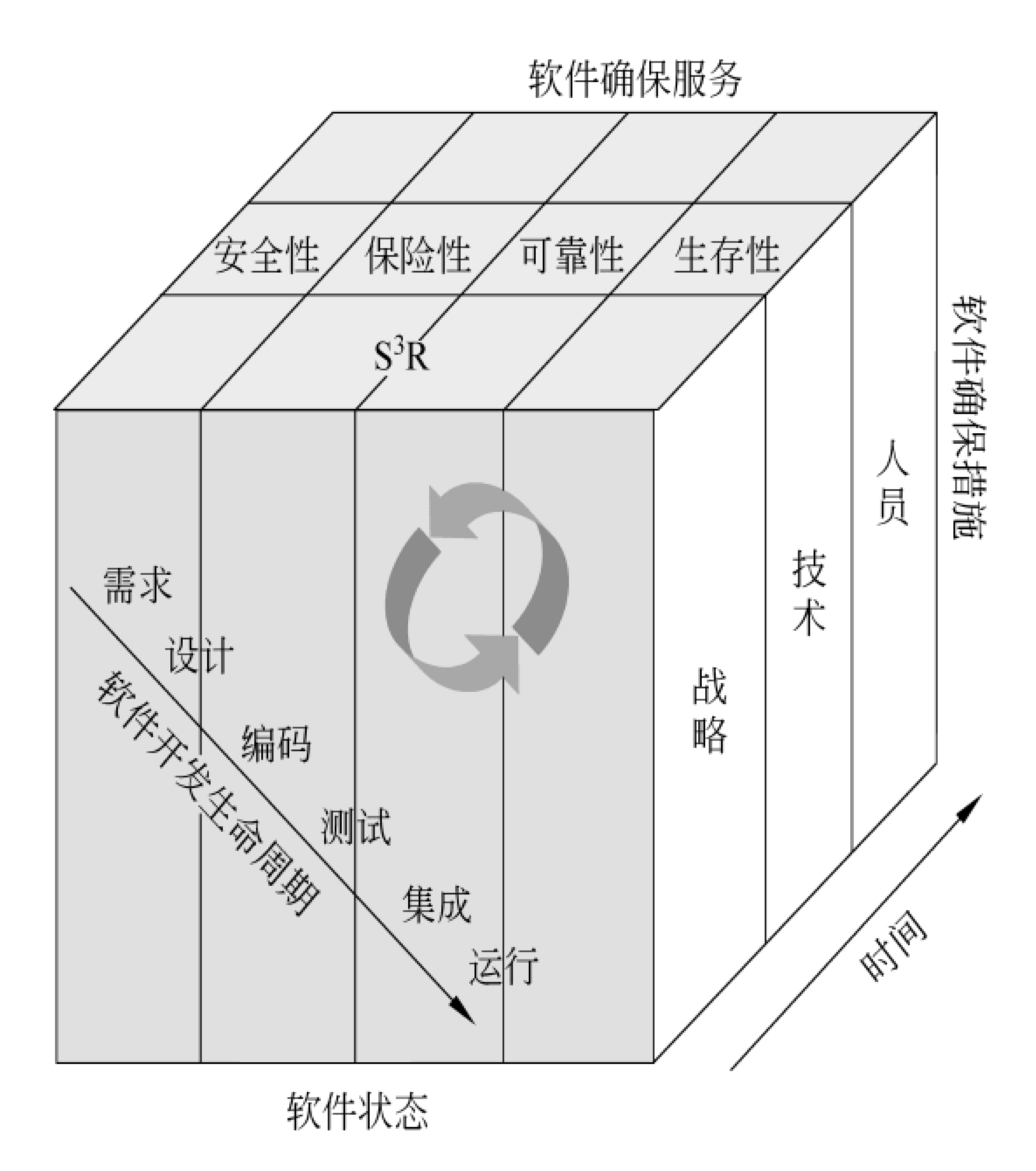


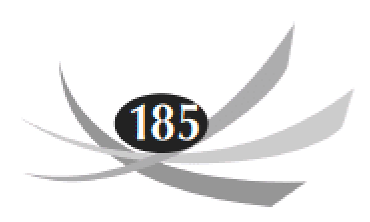
图 7-6 S³R 软件确保模型［FBX2009］

S³R在软件开发生命周期各阶段都加入了风险分析和测试等控制措施。风险分析主要针对需求、设计、测试等阶段，它所关心的主要因素有：风险、威胁、弱点、资产、攻击模式和发生的概率等。从攻击者、资产所有者和软件三个角度对软件进行攻击建模、威胁建模和分析。与传统的软件开发需求不同，S³R更加强调安全性需求工程，需要解决功能性需求和非功能性需求等。S³R结构与设计软件系统容错，常规手段是代码分析，即静态分析、动态分析、故障注入、度量分析、随机数生成分析等。S³R测试主要用于体系结构、设计和开发阶段，其一般基于不同的测试类型进行，同时还关注测试覆盖广度和测试深度、软件组装和集成、认证和鉴定判定是否符合目标要求。建模强调基于模型的安全问题。安全软件设计模型的一个趋势是致力于由设计描述来生成软件，包括：模型风险结构、模型风险开发、模型驱动工程、基于组件的开发，以及Web服务和系统的系统等。并对需求分析、威胁分析、安全策略分析、事务处理与规则分析、性能分析、数据管理分析、因果与风险分析和软件安全确保案例分析等环节建模。基本方法主要包括：数理逻辑、趋势线回归分析、静态模型、流、队列、状态机和模型检测。

在测量与分析方面，S³R重点关注软件确保的4个核心服务的度量与分析，即：

（1）安全性度量与分析：主要是基于各种安全规范进行安全测试，以及针对具体的漏洞、攻击等进行分析。

（2）可生存性度量与分析：主要是基于结构的生存性分析，有基于状态（马尔科夫模



型)和基于路径两种模型。

(3) 可靠性度量与分析：包括黑盒可靠性分析、二项式分布模型、泊松分布模型、基于软件度量的可靠性分析(如分类与聚类)。

(4) 保险性度量与分析：包括概率模型、随机模型、故障树分析、模型检测、自动 Petri 网、时序逻辑等。

S^3R 的程序设计语言与分析包括：面向安全的程序设计语言、软件中安全属性的验证、安全增强机制的自动导入与验证、模型驱动安全方法、发掘安全脆弱性的程序分析技术、基于编译的安全技术、增强信息流与访问控制安全策略等[FBX2009]。

7.4.2 Microsoft SDL

美国国家标准与技术研究院(NIST)估计，如果是在发布后执行代码修复，其修复成本相当于在设计阶段执行修复的 30 倍。因而，越早在开发生命周期发现并修复漏洞，越有可能降低软件开发的总成本。为避免攻击者插入漏洞和降低开发成本，微软在 2002 年提出了安全开发生命周期 SDL(Security Development Lifecycle)模型。SDL 是一套完整而实用的方法，可以降低软件产品和服务中的漏洞的数量，从而减小攻击者攻击供应链系统的几率。目前，微软 SDL 已成为一门成熟的方法学[Microsoft]。

简言之，微软的 SDL 定义了一系列以安全性为主的活动(如图 7-7 所示)，并分布到软件开发的各个阶段中。实施 SDL 的一个必要条件是安全培训，通过培训才能提高安全意识。开发人员是实施 SDL 的核心要素。无论多好的开发流程，如果开发人员不采纳，那该流程也毫无用处。所以，使开发人员具有安全意识是重中之重。对开发人员的培训可从两方面着手，即掌握基本安全知识和改变观念，加强安全意识。对任何政策的实施都要因地适宜，从而应有针对性地对开发人员培训，如设计人员应学会分析威胁；编程人员应跟踪代码中每字节数据、质疑所有关于数据的假设；测试人员应密切关注数据的变化。

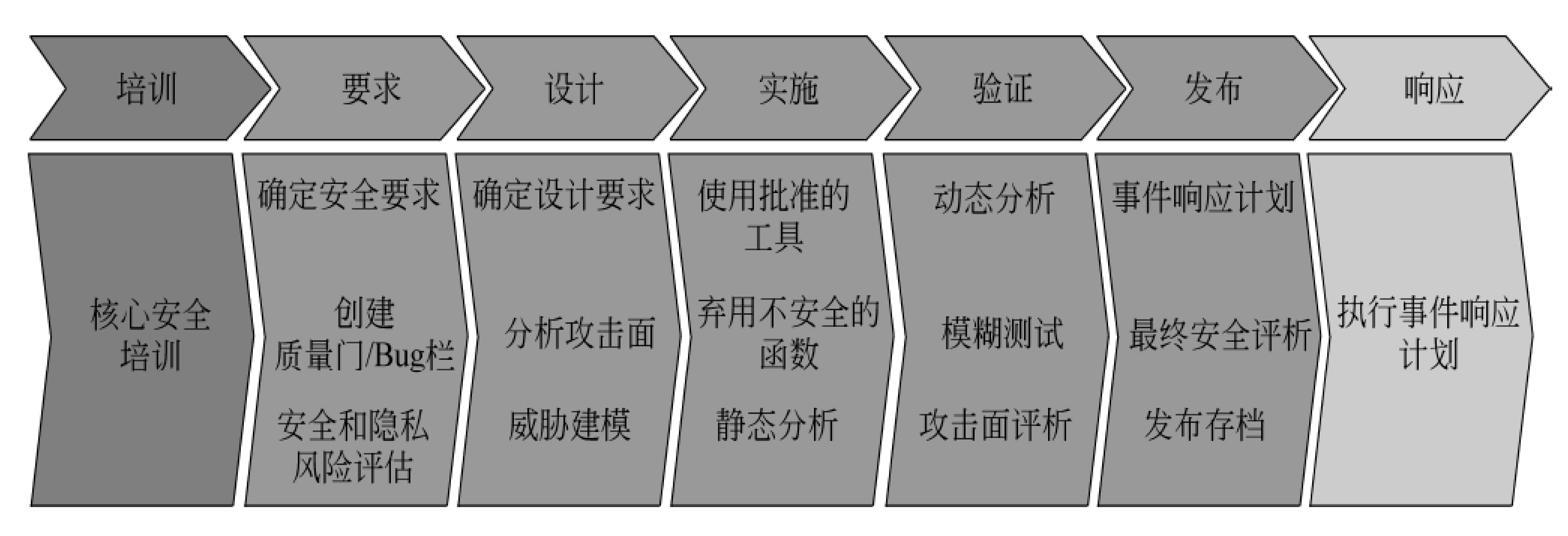


图 7-7 简化的 SDL[Microsoft]

在开展完安全教育培训后，SDL 的过程可顺利展开。大体上，SDL 可分为 6 个阶段：需求、设计、实施、验证、发布和维护。

1. 需求

项目初始阶段是开发团队考虑安全和隐私问题，分析如何使质量和监管要求满足成本和业务需要的最佳时机。在此阶段，一般有 3 项安全活动，即安全要求、质量门/Bug 栏及安全和隐私风险评估。

(1) 安全要求。在项目初期,分析安全和隐私要求,并确定应用程序在运行环境中运行所需的最低安全要求,随后确立和部署安全漏洞跟踪系统。

(2) 质量门/Bug 栏,用于确立可接受的最低安全和隐私质量要求。Bug 栏用于定义安全漏洞的严重性极限值。

(3) 安全和隐私风险评估,该评估用来确定软件中需要深入分析的功能环节。

2. 设计

设计阶段是一个围绕设计、功能规格和执行风险分析来解决整个项目中的安全和隐私问题建立最佳实践方法的关键阶段。该阶段一般包含 3 个安全活动,即设计要求、减小攻击面和威胁建模。

(1) 设计要求。项目生命周期的早期阶段是影响项目设计信任度的最佳时期。在设计阶段,应仔细考虑安全和隐私问题。如果在项目生命周期的开始阶段执行缓解措施,则缓解安全和隐私问题的成本会低得多。项目团队应避免在项目快收尾时才引入安全和隐私功能及缓解措施。

(2) 减小攻击面,指通过减少攻击者利用漏洞的机会来降低风险。

(3) 威胁建模。利用威胁建模技术建立系统模型。

3. 实施

实施阶段重点在于帮助终端用户对安全部署软件的方法做出明智的决策。这一阶段也是检测和移除代码中安全问题采取措施的时期。该阶段一般包含 3 种活动,一是开发团队尽量使用最新的批准工具,以便使用最新的保护措施和安全分析功能。二是开发人员禁用不安全的函数。三是项目团队对源代码进行静态分析。

4. 验证

验证阶段指确保前期阶段编写的代码满足安全和隐私原则。该阶段包含的安全活动有动态程序分析、模糊测试、威胁模型和攻击面评析。动态程序分析是为保证程序能预期运行而对程序进行的运行时验证。模糊测试是通过故意向应用程序中插入有害数据来诱发程序出错。威胁模型和攻击面分析是确保所有因系统设计和实现的更改而形成的新攻击平台得以评析和缓解。

5. 发布

目前,无论何种软件开发模式都无法保证发布的软件是无漏洞的。因此,需要事先在发布前做好相关工作。发布阶段重在准备公开发行项目,包括执行发布后的维护任务和解决之后的安全漏洞的计划方法。该阶段的安全活动包含制定事件响应计划、在发布之前仔细检查对应用程序执行了所有的安全活动即最终安全评析(FSR),后发布软件的生产版本或 Web 版本,此外,还需对软件的所有相关信息和数据进行存档,以便后期对软件进行维护。

6. 维护

维护阶段重在开发团队能适时地处理报告的软件威胁和漏洞。该阶段主要的安全活动即实施发布阶段的事件响应计划,帮助用户避免出现软件问题,并分发软件更新和授权性的安全指导。

总结 SDL 的特征如下[BDW2008]:

(1) 作为支持质量的安全性：SDL 的主要目标是通过改善安全性状况来提高功能性软件的质量。安全活动主要和功能性建设活动相关。很少关注安全机制的实现和集成。SDL 设计作为软件开发工程的附加部分。

(2) 定义的过程：SDL 过程被良好的组织化，并在各阶段中开发相关的安全活动。而且，在 SDL 过程中，这些活动是连续的，包括威胁模型和教育。因此，SDL 过程支持修改和改善中间结果。

(3) 良好的指导：SDL 在指定用于执行活动的方法方面做得很好，例如通过流程图降低攻击表面，并把威胁模型作为一个更详细的过程来描述。因此，即使对于没有经验的人，也可以执行活动。

2012 年，微软在安全开发大会上公布了 SDL 在关键基础设施保护方面的两个最新成功案例(印度政府和 Itron)，可见，SDL 的应用范围已超出了传统应用程序厂商的范畴。总之，SDL 适合于大型软件、安全性要求较高的软件开发，同时也较适合运作在大型组件、企业上。

尽管 SDL 可以减少软件的安全漏洞，提高软件的安全，但是利用 SDL 开发的软件也不能完全避免安全漏洞，如 Windows Vista 就是严格按照 SDL 开发的，但是它依然存在安全漏洞。

7.4.3 OWASP CLASP

CLASP(Comprehensive，Lightweight Application Security Process)即全面的轻量级应用程序安全过程，是由 OWASP 开发的安全软件开发生命周期方法，简言之，就是一个开发安全软件的轻量级过程。顾名思义，CLASP 是轻量级的，它易于使用，且非常有效。而且 CLASP 不如 SDL 对安全性的需求那么严谨，从而其较适合于轻量、安全性需求不高的小组织。CLASP 提供了一种尽早在软件开发生命周期的早期阶段关注安全问题的好的组织和结构化方法。实际上，它是一组可集成到软件开发生命周期中的过程的片段。CLASP 采用说明性的方法，记录组织的活动，并为合理实施这些安全活动提供广泛的安全资源。

CLASP 由一个以活动为中心、角色为主的元件组成。在软件开发过程中，其提供了许多最佳实践方法供开发人员参考，而且还可将一个有组织、可重复使用、并且可测量的方法运用到现有或新的软件开发流程中。从整体的架构来看，CLASP 可分为三大部分：CLASP 视图、CLASP 资源和脆弱性用户案例[DG2006]。

1. CLASP 视图

CLASP 可从概念、角色、活动评价、活动实现和脆弱性五方面来分析，称为 CLASP 视图，这些视图帮助开发人员快速理解 CLASP 的流程，例如明确各元件如何交互，及如何将元件应用到特定的软件开发生命周期中。

(1) 概念视图，对 CLASP 简单地做一个整体性介绍，例如介绍了 CLASP 的五个视图之间的联系(如图 7-8)、7 个最佳实务、CLASP 分类、安全政策间的关系以及应用 CLASP 流程组件的顺序。

(2) 基于角色的视图，定义了角色(项目经理、架构师、开发人员、安全核查人员等)在

CLASP 流程中的关系。有效的安全性实践需要组织积极地投入,因而 CLASP 划分了角色及其相关责任。

(3) 活动评价视图,帮助项目管理人员评价 24 种安全相关的活动,并选择一个活动子集,因为项目没必要全部采用 CLASP 中的每一个活动,只需要针对目前组织的弱点进行加强或改进。CLASP 提供了两个简单的例子(如遗留的或新开始的)帮助选择可应用的活动。

(4) 活动实现视图,定义了 24 种安全相关的活动,并指出了这些活动的执行者。CLASP 的这些活动阶段把活动评价视图中评估和接受的活动子集转化成可执行的软件。

(5) 脆弱性视图,从源码含有的漏洞着手,CLASP 分出了 104 个问题类型,一种问题类型往往不是一个安全漏洞,而是引起源码中安全漏洞的安全条件的问题组合。而且,脆弱性视图说明了在问题发生时,采用何种技术以解决这些问题或降低问题发生时带来的影响。

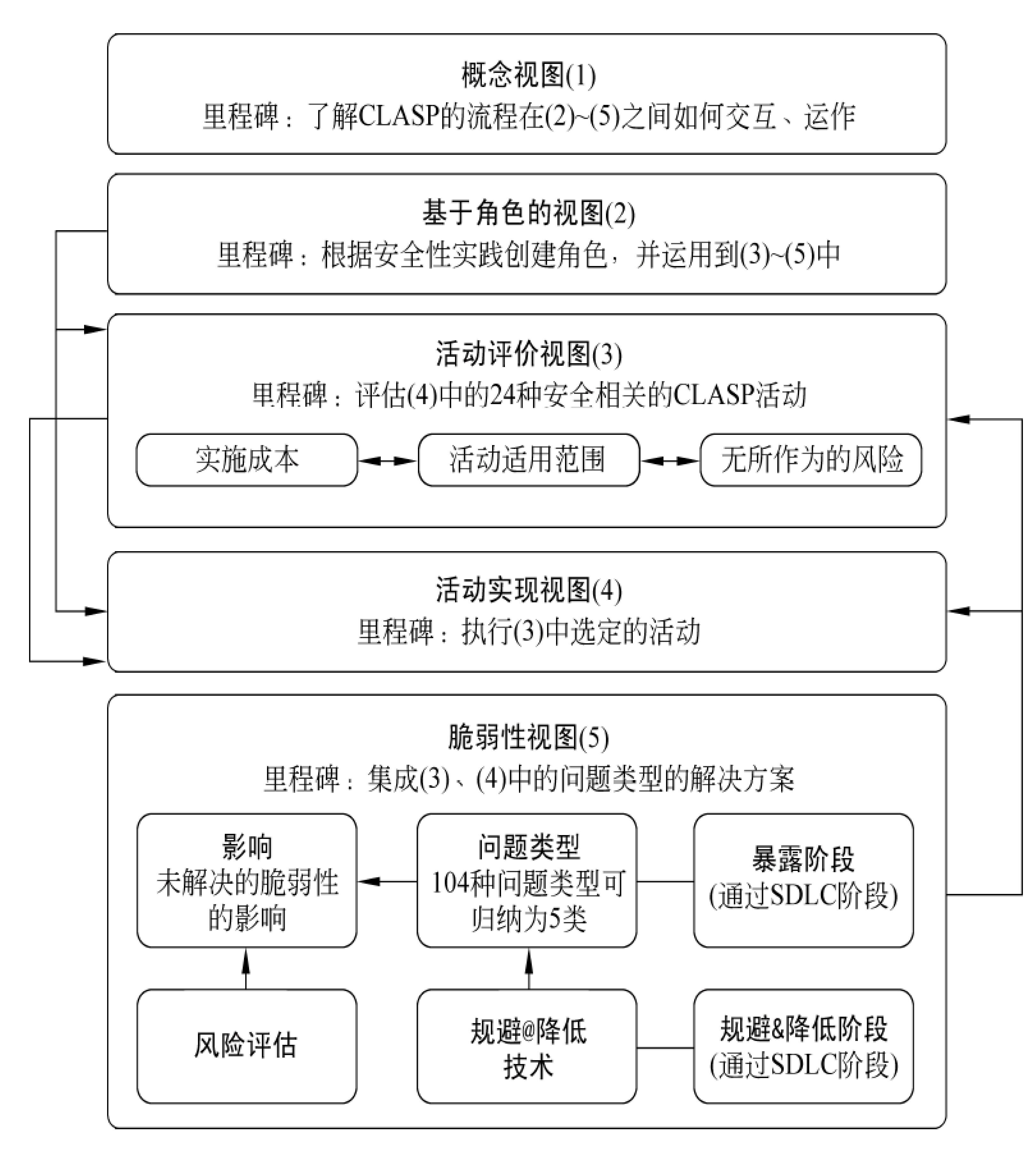


图 7-8　CLASP 的视图及其交互[DG2006]

2. CLASP 资源

CLASP 资源可帮助项目经理和开发人员计划、执行活动等,例如,完成编码指导工作表有助于项目经理明确哪些问题类型会对构建软件系统带来风险。反过来,这可助于决定哪些 CLASP 活动必须执行。一些 CLASP 资源对使用工具来自动化产生 CLASP 流程组件的项目极其有用,这些资源如下:①应用程序安全的基本原则,如最小化攻击平

面、不安全的引导原则、深度防御等。②重要的安全服务和概念的描述。对于一个系统，拥有许多的安全目标，如访问控制、数据完整性、可用性、机密性和不可否认性等。③系统评估工作清单，如开发过程和组织、系统资源、网络资源使用的详细情况等。④蓝图样本。新计划提供的样本是让组织使新开发流程处于安全的软件开发流程中；而原有的计划提供的样本是让组织在现有的开发流程中仍能进行 CLASP 的活动。⑤安全专业术语。⑥制定开发过程计划。⑦组织流程开发团队，把开发团队的流程整合进 CLASP 流程中，通常组成流程开发团队最有效的方法就是从开发团队中挑选人员，让他们拥有制定流程的控制权。

3. 脆弱性用户案例

CLASP 的脆弱性用户案例与脆弱性视图相关联，它可让用户简单了解在哪些环境下，攻击者使用哪些服务会给应用程序带来哪些威胁。例如，用户案例以易于理解的方式让 CLASP 用户明白因无安全意识设计编码而可能导致的安全服务方面(如授权认证、保密性、可用性和不可否认性)的漏洞。

总结，CLASP 的重要特征如下[BDW2008]：

(1) 中心阶段的安全性：CLASP 的主要用于支持安全性为主的软件开发。CLASP 主要从安全性-理论性角度来定义和构思活动，因此，一系列活动的范围相当广泛。

(2) 没有过程：CLASP 是一系列集成于开发过程和操作环境的独立活动。为了灵活性，选择执行的过程和执行的顺序是开放的。而且，每个个体活动指定活动的执行频率，导致了复杂的协调。定义两个路线图(遗留的和新建的)，为如何结合这些活动到一个连贯的和有序集中提供指导。然而，这不是一个集成的过程。

(3) 基于角色：CLASP 定义了角色，并为这些角色分配相应的活动。角色可以影响软件产品的安全状况。因此，从另一个角度审视，角色可用于构建一系列活动。

(4) 丰富的资源：为帮助实施活动，CLASP 提供广泛的安全性资源。其中的一个资源是 104 种已知问题类型的列表，这些问题类型可构成应用程序代码中安全漏洞的基础，还可在代码审查时作为检查列表。

像 SDL 一样，CLASP 强调安全测试的重要性。但是，与 SDL 相反，CLASP 更加注重于白盒测试。此外，CLASP 没有优先级排序。

7.4.4 Touchpoints

接触点模型(Touchpoints)是由 Gary McGraw 提出的应用在不同的软件工件中的最优安全开发方法。Touchpoints 是基于多年来收集的行业经验，从而确保提议的安全活动具有可行性。它提供了一组最佳实践方法(又称为活动)，将最佳实践方法大致分为七类，即接触点。图 7-9 详细说明了软件安全接触点，并指出了在软件开发过程中，开发人员应如何将这些接触点应用到不同的软件工件中。尽管图中工件的顺序类似于瀑布模型，但是现在大多数的开发过程都在遵循某种迭代方法。因此，接触点在软件开发生命周期中将被迭代使用。根据有效性，接触点的排列顺序为：代码审查、架构风险分析、渗透测试、基于风险的安全测试、滥用案例、安全需求和安全操作[GMG2006]。

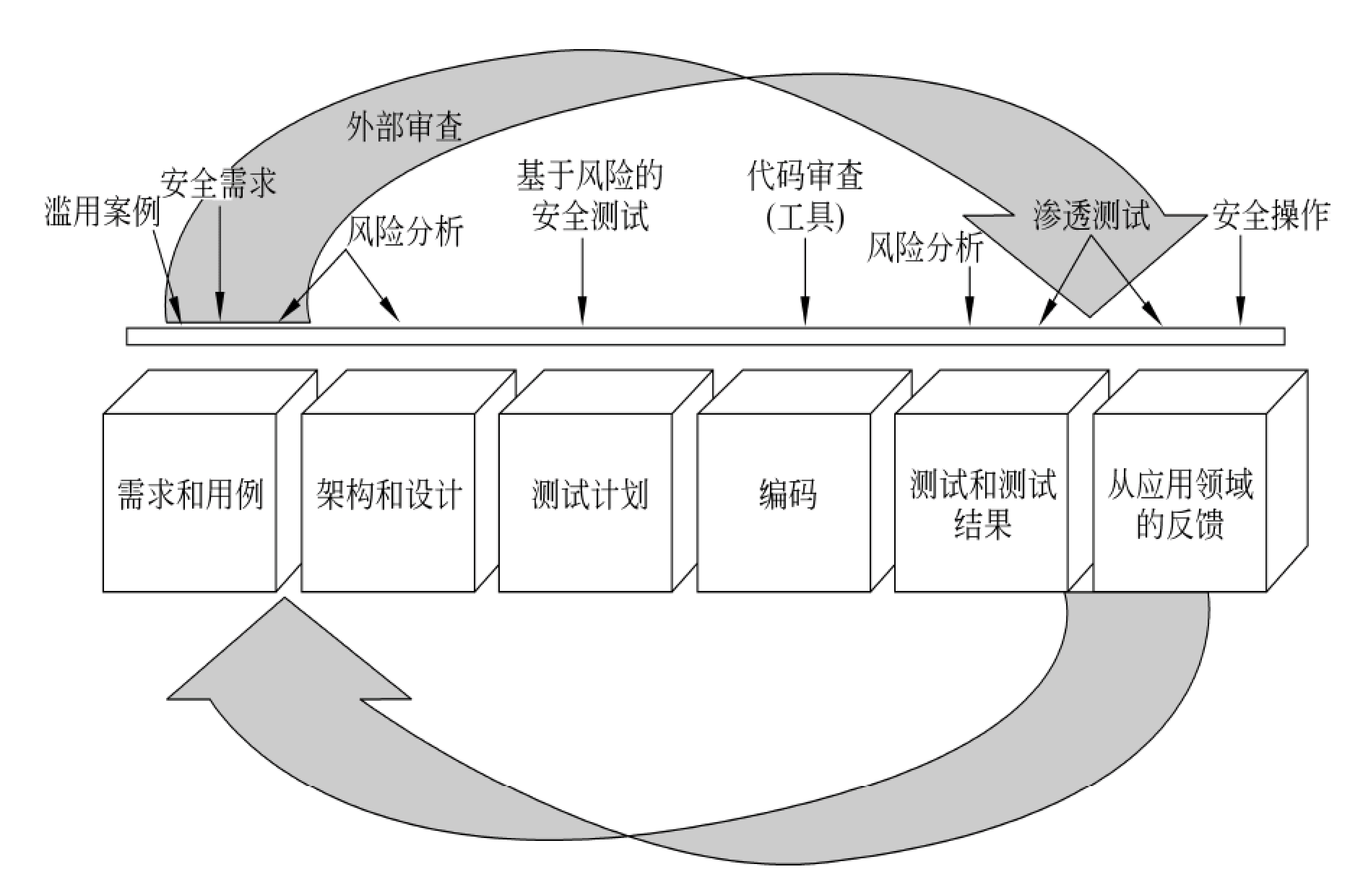


图 7-9　接触点模型[GMG2006]

1. 代码审查

代码审查是通过阅读源码来检查代码是否符合编码标准及相关的质量活动，旨在发现及修正软件开发初期未发现的漏洞，例如不恰当地处理输入、缓冲区溢出和异常处理等。代码审查是一种实现安全的软件的必要而不充分的方法。其针对的工件是代码，可借助静态分析工具等进行审查。

2. 架构风险分析

架构风险分析旨在找到瑕疵。在很多情况下，代码审查和架构风险分析的执行顺序可互换。架构风险分析针对的工件是设计和说明书。在基于说明书的体系结构阶段和类层次的设计阶段，架构风险分析都是不可或缺的。安全分析人员在此阶段需揭示架构瑕疵，评级瑕疵，并开始进行降低风险的活动。

3. 渗透测试

渗透测试是针对系统威胁试图对系统进行渗透，发现系统最薄弱的环节。其测试可分为两种，一种是旨在验证软件正常执行了预期的任务；而另一种是依据 CVE(Common Vulnerabilities and Exposures，通用漏洞披露)已经发现的安全漏洞和缺陷，模拟攻击者对系统进行非破坏性的攻击性测试，以便确定系统在攻击之下的反应情况。渗透测试针对的工件是处于环境中的系统。其有助于很好地理解实际部署的软件在真实运行环境中的运行情况。

4. 基于风险的安全测试

基于风险的安全测试旨在揭示可能的软件风险和潜在攻击。其针对的工件是单元和系统。基于风险的安全测试更依赖于专门的技术和经验，而不是测试经验和安全经验，可使测试人员学会从攻击者的角度去测试系统。

5. 滥用案例

滥用案例指软件开发人员除了考虑正常特性外，还需思考软件系统的固有特性，如可

靠性和安全性。其模仿攻击者思考系统,并利用“反需求”尝试出错点从而事先预测系统可能出现的异常行为。滥用案例针对的工件是需求和使用案例。类似于使用案例,滥用案例描述了系统在遭遇攻击时的行为表现,构建滥用案例要求明确地说明应该保护什么,免受什么来源的攻击,以及保护多长时间。

6. 安全需求

设计系统的安全需求,必须明确地在需求中加入安全考虑。好的安全需求包括明显的功能安全(如应用加密)和紧急特性(滥用案例和攻击模式可以很好地捕获它们)。由于确定和维护安全需求的方法错综复杂,所以要灵活地处理这些方法。

7. 安全操作

安全操作针对的工件是实际部署的软件。安全操作允许和鼓励网络安全专业人员积极应用接触点,提供开发人员可能缺乏的经验和安全智慧。例如,在开发和维护过程中,不可避免地需要更改配置,为保证其安全性,我们需要验证配置的任何修改,防止恶意修改配置。总之,在增强系统的安全状况的过程中,经验丰富的操作人员应认真地设置和监视部署的系统。

然而,无论设计和实现的力度如何,仍会出现攻击。因而,理解导致攻击成功的软件的行为是一种重要的防御技术,将通过分析攻击行为而获得的知识再应用到软件开发中。

总结,Touchpoints的特征如下[BDW2008]:

(1) 风险管理:当谈及软件安全时,Touchpoints承认风险管理的重要性。它试图通过详细说明支持接触点活动的风险管理框架来提高软件安全。

(2) 两面性:接触点提供混合的正反面活动,这两种活动有助于产生有效的结果。正面活动(如代码审查)在控制、功能性方面更具有建设性,反面活动(如渗透测试)是关于攻击、破坏软件等的活动。

(3) 灵活性:不同接触点的优先级有助于公司从最重要的部分逐渐引入接触点。

(4) 案例:Touchpoints富有案例。例如,当描述滥用案例时,具体的案例可以让读者很好的了解在特定情形下,程序如何反应。

总之,软件安全工程从软件开发生命周期的角度对软件开发的每一个阶段都加以安全因素考虑。

7.4.5 OWASP SAMM

软件保证成熟度模型(Software Assurance Maturity Model,SAMM)是一种帮助组织制定并实施软件安全策略的开发模型,该模型旨在解决组织所面临的特定的软件安全风险。SAMM提供的资源可用于评估一个组织现有的软件安全活动,并建立一个迭代的平衡的软件安全保证计划,后证明该计划可带来的实质性改善。此外,还可用于定义并衡量组织中与安全相关的措施[OWASP]。

SAMM定义灵活、应用广泛。无论是何种规模的组织(大、中、小型组织),还是何种类型的软件开发,都可使用该模型。

1. SAMM 的内容

SAMM 建立在软件开发的核心业务功能的基础上。如图 7-10 所示，SAMM 在最高级上，设置了四种关键业务功能：监管、构造、确认和部署。每种业务功能是一组软件开发过程中具体细节的相关措施，简而言之，任何软件开发组织必须在一定程度上实现每一个业务功能。

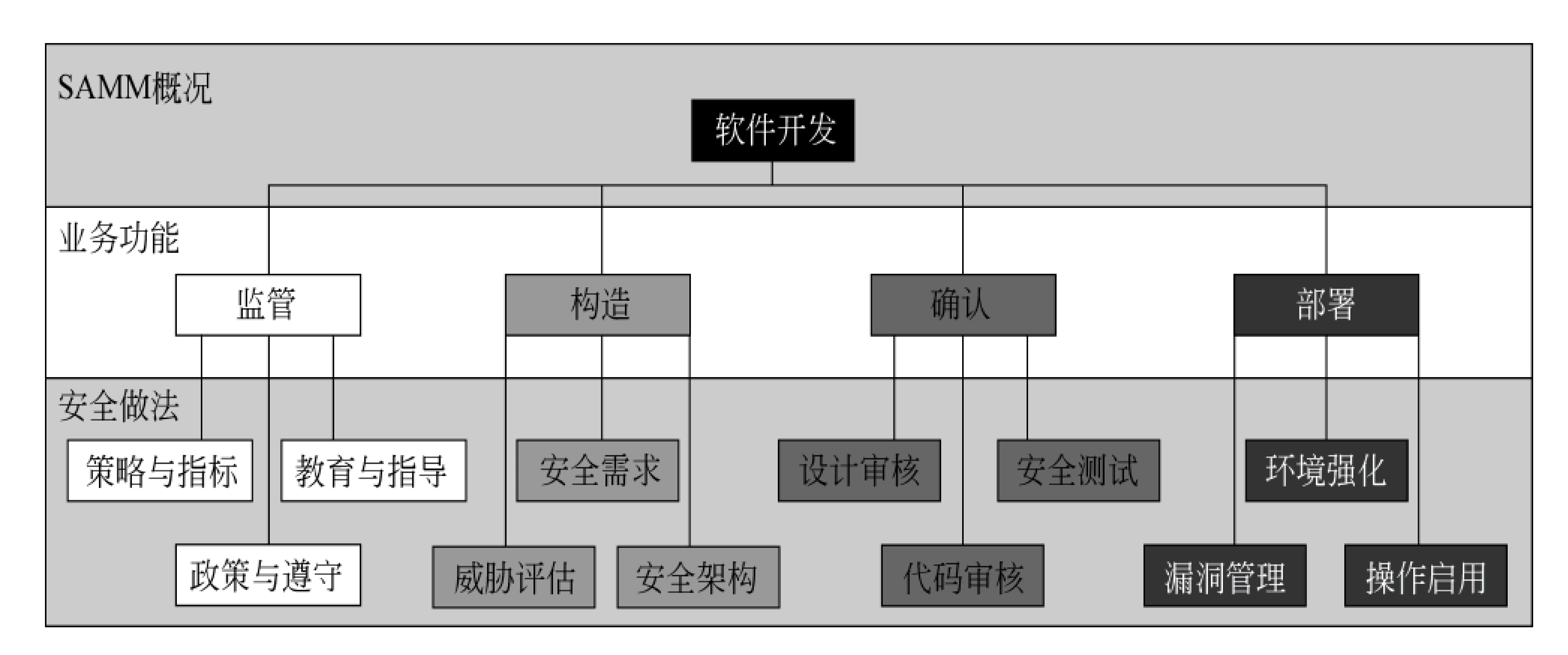


图 7-10 SAMM 概况[OWASP]

鉴于业务而只是针对这 4 方面，而没有与安全直接相关的内容，SAMM 针对每一个业务功能设置了三种安全做法(SAMM 的基础)。每种安全措施都可视为一个与安全相关的措施的领域，从而为相关的业务功能建立安全保证。从总体上看，这十二个安全措施都是改进软件开发业务功能的独立部分。

而且，为证明组织是如何随着时间而改变的，SAMM 对十二个安全做法都设置了三个成熟度等级作为目标。安全做法中的每个等级，通过设置比先前等级更严格的成功指标和特定的活动，设定一个了更加复杂的目标。

(1) 监管。监管集中于组织如何管理所有软件开发相关的处理过程和措施，如关注多组人员共同研发的过程。

针对监管，设置了策略与指标、政策与遵守和教育与指导三种安全活动。策略与指标集中于为软件安全保证计划在组织中建立一个框架，包含总体战略方向和采集一个组织安全态势的测量处理过程和措施。政策与遵守集中于理解并符合法律等规章制度和内部安全标准的要求，以及项目级别的审计。教育与指导集中于通过为员工提供培训以及与安全相关的信息指导，来提高项目团队的安全认识。

(2) 构造。构造集中于组织对于开发项目中设置目标和创建软件相关的处理过程和措施，主要包括产品管理、收集的需求、体系结构说明、详细设计和执行。

针对构造，设置了威胁评估、安全需求、安全架构三种安全活动。威胁评估集中于识别一个组织的软件中潜在的攻击，以便更好地了解风险。根据每个项目的威胁和潜在的攻击的详细信息，组织通过对安全措施的优先次序，有效地做出更明智的决策。安全需求集中于在软件开发过程中，在开始阶段除明确指定正确的功能外，还须指定与安全相关的预期行为。安全架构集中于在默认的情况下，组织可采取的促进安全设计的措施，和在软件开发过程中对所有技术和构架的控制，以支持设计过程。

(3) 确认。确认集中于组织如何检查和测试软件开发过程中中间产品相关的处理过程和措施,主要包括质量保证工作,如测试等。

针对确认,设置了设计审核、代码审核和安全测试三种安全活动。设计审核集中于针对与安全相关的问题评估软件设计和架构,进而使组织能较早检测到架构层面的问题,从而避免因安全问题而导致后期重构所带来的潜在昂贵成本。代码审核集中于对软件的源码进行检测,以帮助发现安全漏洞及相关的弥补措施,并建立一个安全编码的最低期望值。安全测试集中于在运行环境下测试软件,以发现安全问题,并为软件发布建立一个最低预期。

(4) 部署。部署集中于组织如何管理软件发布相关的处理过程和措施,主要包括将产品发送给终端用户、在内部或外部主机上部署产品,以及运行时软件的正常操作。

针对部署,设置了漏洞管理、环境强化和操作启用三种安全活动。漏洞管理集中于管理内部和外部的漏洞报告,并建立一个一致的处理过程。环境强化集中于为软件的运行环境建立保证。操作启用集中于将软件开发过程中关键的安全信息提供给用户和操作人员,以帮助用户正确配置、部署和运行软件。

总之,SAMM 定义了一个组织可以进行的各种安全活动,并使用循序渐进的方法来逐渐降低安全风险和加强软件的安全保证。每一个安全做法可视为一个成熟度领域,若该领域达到了某个成熟度等级,则表明该领域已采用了一系列的相关安全活动。简而言之,就是阶梯式地改善软件安全保证计划:先选择改善安全保证计划下一步所需执行的安全活动,然后执行该活动。执行完毕后,判断是否已达到成熟度等级的衡量标准,若符合标准,以此来明确改善保证计划的下一个目标。

2. SAMM 的应用方法

组织可把 SAMM 作为度量标准来衡量安全保障计划,并创建记分卡。通过使用记分卡,组织能够验证通过迭代执行一次安全活动来不断改善保证计划。而且,组织还可使用路线图模板来指导建立或完善一个安全保证计划。

目前,SAMM 的开发公司(Fortify 公司)已为 20 多家公司对如何使用 SAMM 做了指导。据估计,目前全球有 50 多家公司使用 SAMM 来帮助建立他们的安全保证计划。

3. SAMM 与 SDL 的异同点

共同点:SDL 和 SAMM 都注重源码分析,并鼓励使用自动化工具。但是都没有直接解决安全配置管理问题。

不同点:首先,从模型内容上而言,SAMM 内设等级制度,可以使公司决定采用何种级别的措施来改善单个安全实践。尽管 SDL 的优化模块有向类似的方向改进,但是 SDL 目前没有这一等级功能。

其次,从应用范围上而言,SAMM 没有 SDL 的应用范围广泛。SAMM 适合于以自主研发为主的软件公司或机构(如金融机构),而 SDL 更适合于以软件开发为主的公司。例如,银行通常在开发一个漏洞补丁后,只需通知系统管理员安装该补丁。而微软在开发完一个补丁后,通常需要分发给广大用户,让用户自行安装。从风险暴露的层面上讲,后者引起的风险远远大于前者。因而,以那些以非软件开发为主的公司或机构使用 SDL 会比较困难。

7.5 软件供应链的强化策略

软件供应链本身是一种供应链，所以现有的供应链的安全策略可选择性地应用于软件供应链，在此不再赘述。但是，软件供应链又具有特殊性，因为其传输产品是软件，以下简单介绍一些加强保护软件供应链安全的策略。

7.5.1 降低开发风险

1. 软件代码监管

不安全开发过程中的风险或者攻击者，可能通过全球供应链中的联系破坏软件产品的安全。在开发人员编码、代码交换或发布时可能引发应用程序安全问题。为应对这类问题，主要的软件供应商应利用软件完整性控制，而且开发人员须建立和使用一组完善的常用安全控制机制。

软件代码管理正是安全控制机制之一，是一套软件开发组织用于定义和测试标准软件策略的管理流程，以确保软件质量的可靠性和安全性，并提高开发效率。对代码实施进程管理，能够让企业更好地对风险进行管理，并更好地配合企业整体商业优先级完成产品开发。

2. 评定软件安全等级

开发一种安全价值的加权指数软件，提高确保指标的有效性。加权评分可以通过测试以下组合生成：实用工具本身如何准确找到漏洞，及能发现多少漏洞；工具代码覆盖的数量；该工具是如何针对软件运行，以及漏洞检查的范围多大。

同时，企业可建立一个应用程序安全计划，深入了解并改善应用程序组合的安全性。

3. 改善通用标准

改善通用标准比开发一个针对特定部门的新方案变得更容易和更有效。现有的通用评估准则(CC)可用来评估商用产品的保障性问题，但是通用评估准则目前无法完全评估某些特殊部门(如国防部)所用软件产品的可信度，特别是评估保障 4 级及以下等级时并不执行渗透测试[DSB2007]。因而，不断改善通用标准，并使只有通过通用标准认证的 COTS 软件可以被用到国家安全的 IT 系统上，那么软件系统的安全性将会大大增强。

7.5.2 软件安全测评

1. 软件安全保障测评

软件安全保障测评(如图 7-11)是指对软件的整个开发生命周期进行全面、综合分析，查找需求、设计、实现等各个阶段中存在的安全缺陷和隐患，并对这些安全缺陷和隐患进行深入分析，给出修复建议，在确认这些安全问题修改完善后，最终综合评定其安全保障级别的过程。

软件安全问题的主要原因是在软件开发生命周期的各个阶段存在安全缺陷。保障测评通过进行全面的软件安全缺陷测评，能够极大的提高软件的安全性，促进软件开发的可

控性和规范性。

2. 软件源代码漏洞分析

就软件而言,漏洞就是劣势,漏洞造就了软件的脆弱性,进而造成了软件供应链的脆弱性。和其他工程一样,这种缺陷源于系统设计或实施过程,但其又是不可避免的,甚至是意料之外或者蓄意制造的。蓄意制造的漏洞一般隐藏的都比较好,对于那种大规模的软件来说,漏洞审查的大部分注意力都集中在那些意料之外的缺陷上,而且对这种漏洞的审查成功率也比较高,因为没有什么障碍物干扰审查,相反,要想发现那些深藏不漏的恶意制造的漏洞就不这么简单了,从而需要使用软件源代码漏洞分析技术。

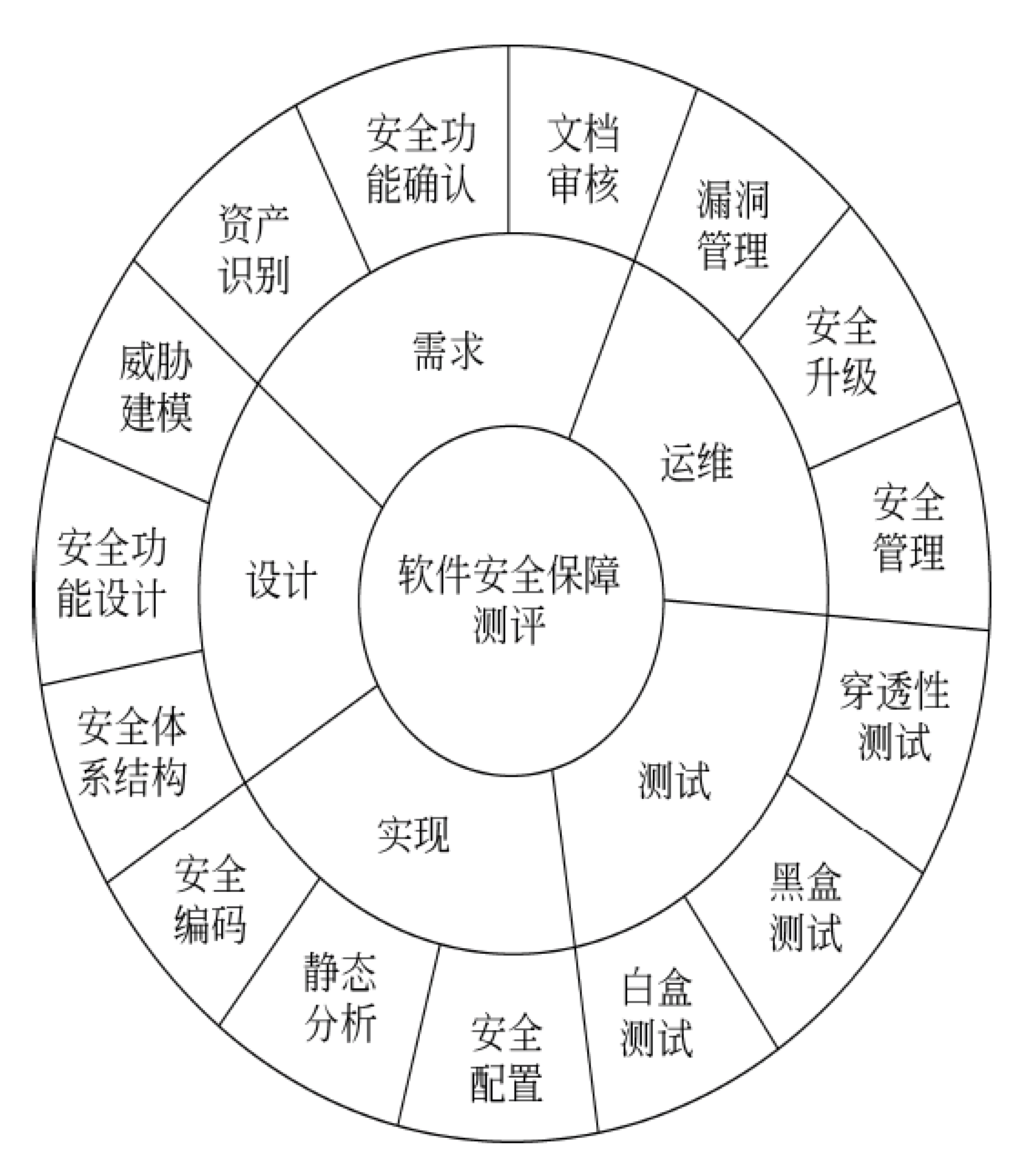


图 7-11 软件安全保障测评

软件源代码漏洞分析(如图 7-12)是指对软件源代码安全性进行全面分析,查找源码中存在的安全缺陷和隐患,并对这些安全缺陷和隐患进行深入剖析,综合评估其可能造成的安全风险,最终给出修复建议的过程。

源代码是软件的“原材料”,对源代码进行安全分析意味着守住了软件安全最关键的安全防线之一。通过源码漏洞分析可以帮助用户从根源上减少 30%~70%的软件安全问题。只有源代码中的安全缺陷得以及早消除,最终形成的软件产品才能具备较高的安全性,有效降低整条软件供应链的安全风险。

3. 软件定制漏洞分析

软件定制漏洞分析(如图 7-13)是指在服务期限内对客户指定清单中的软件进行自主漏洞分析,在第一时间通过专用的漏洞预警平台,采用专用客户端、手机短信或电子邮件等多种方式为用户提供清单中软件的定制化安全漏洞预警,内容包括软件漏洞信息和相应的漏洞消控解决方案。

软件中的漏洞,就像攻击者自由出入客户信息系统的“大门”,是导致 ICT 系统安全事件频发的主要根源。目前,解决软件漏洞最主要的技术手段是打补丁,缺乏时效性,而

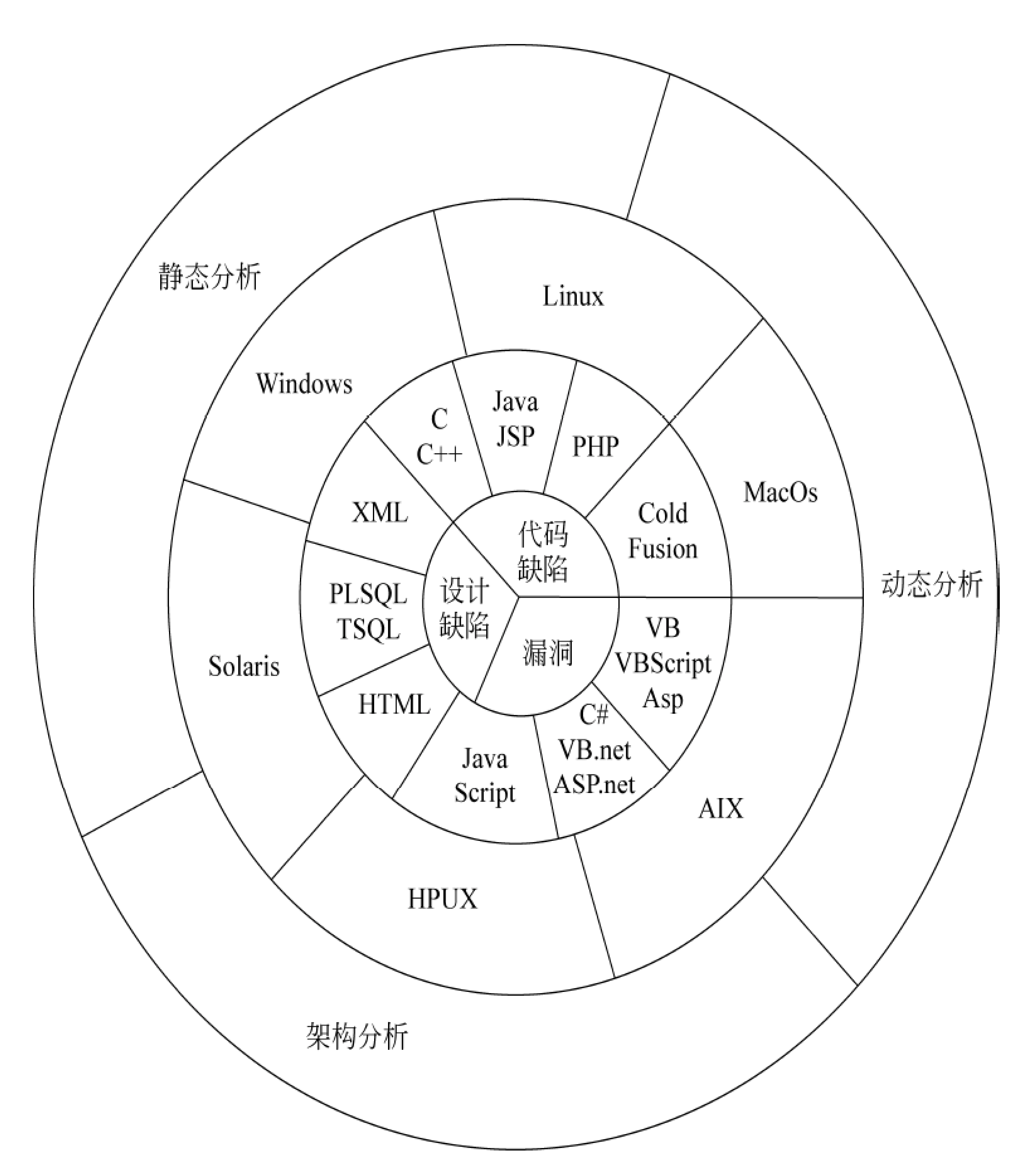


图 7-12 软件源码漏洞分析

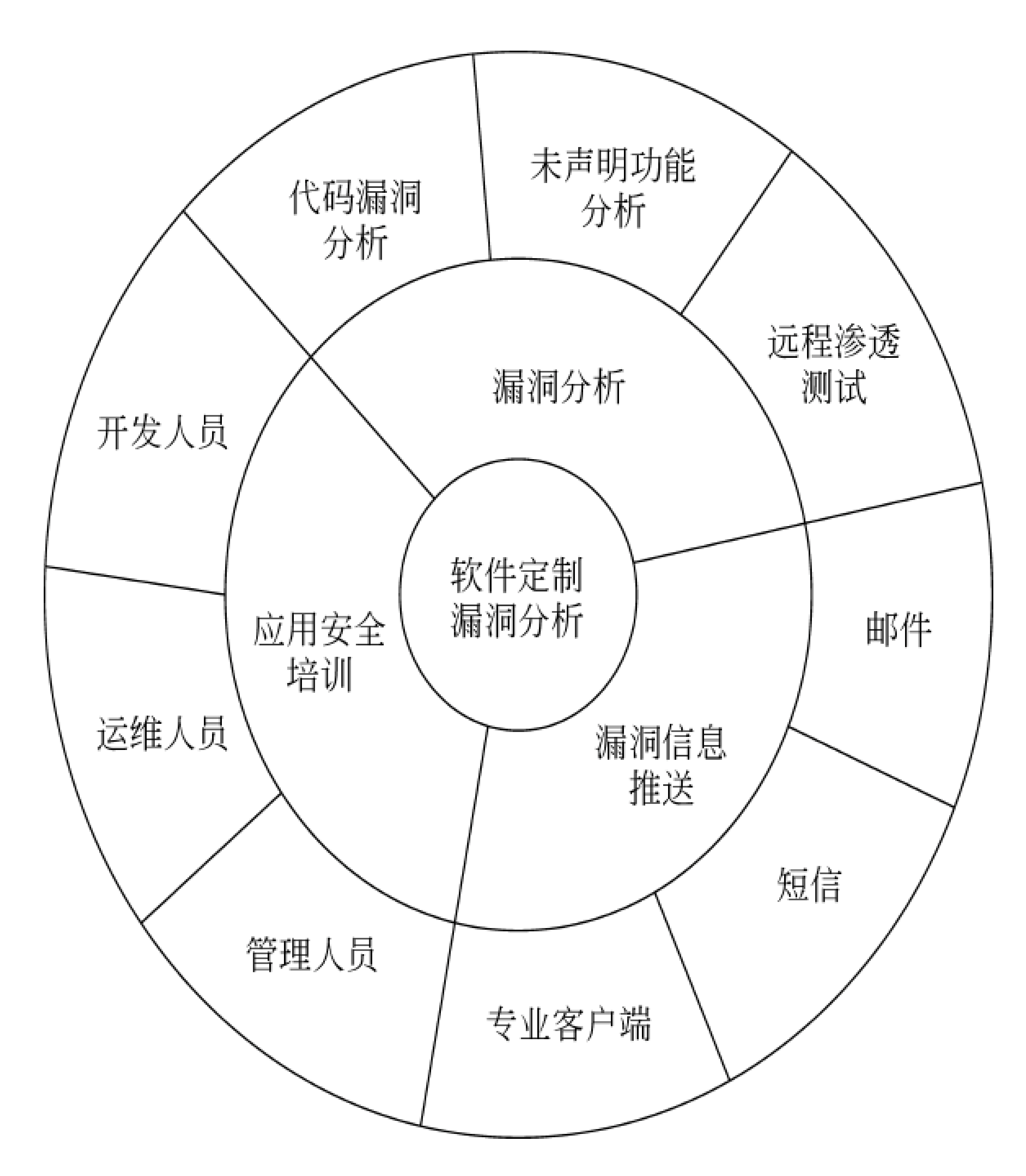


图 7-13 软件定制漏洞分析

且众多中小规模软件开发厂商基本不提供补丁分发机制，因此传统的事后打补丁机制不能满足重要信息系统的安全需求。通过软件定制漏洞分析，用户可以对ICT系统中的软件进行精细化、专业化的安全管控，及时发现并修补安全漏洞，从根源上减少安全问题，降低软件供应链的安全风险。

7.5.3 可行性举措

1. 鼓励创新

创新为经济和军事活动开发新产品、新服务或新的生产方式。创新提供了思想流动，同时也为安全提供了重要的优势。增强创新能力的政策可以降低全球化中软件供应链的风险，比如降低使用国外软件（或者其他IT产品）带来的风险。这个假设的对立面是绝对正确的。如果国家不加强创新能力，不管他在软件保障里花费多少心血，即使建立新的评估的程序，他的软件系统也无法确保安全。因为更少的创新意味着更多的新产品会来自国外，来自未知的源头，从而对这些产品知之甚少，对其隐患更加无措。总之，任何加强安全的策略都必须包含提高创新的政策[JAL2007]。

2. 提高采购软件的总体质量

采购商可通过提高其采购软件的总体质量来提高软件攻击的“信噪比”。如果软件本身存在很少的无意错误，恶意软件就更容易被发现。尽管信息保障（IA）的普遍改善本身无法阻止对软件供应链蓄谋的攻击，但提高商用现货软件的总体保障/安全可信度还是可以带来令人瞩目的好处。现如今还没有针对软件开发过程进行评估的制度，也没有保证软件开发商能产生有效可靠的软件制度，因此采购商对软件供应商提出的安全保证方案主要是制定一个能正确评价供应商软件开发能力和保证软件安全的制度，以此来了解和评估软件供应商生产安全软件的能力[DSB2007]。

3. 供应商的诚信度审查

目前，供应商的诚信是一个受质疑的问题，为此，需要建立可信的供应商源。通过查出供应链上的受污染环节保证软件系统免受贪污的侵蚀。无论机密资料有否透露给供应商，这种供应链上的风险都存在。从保证系统的角度看，供应商的诚信度审查主要是用外部渗透的方式，通过对抗控制并影响着商业或工程的进程及其能够发挥的作用。此外，根据审查情况，结合供应商软硬件所有源头信息建立国家信息交换中心，以加深政府对于在采购中使用的特定供应商关联风险的了解。如有必要对软件供应链进行系统的反间谍审查时，也可以借用这些相关信息来参考[DSB2007]。

4. 政府可采取的措施

更好的管理有一个至关重要的因素，即更集中的政府政策来保证努力的一致性。政府应该在协调和引领提升软件安全性上扮演重要的角色，充分利用一些最好的商业尝试。这些尝试包括对编程人员的安全意识培训，在设计软件之初就将安全因素考虑其中，对总体监控和透明操作有强有力的管理，包括对代码的更改和添加上的监管，后期在安全问题上独立的再检查（包括使用自动检查软件）等。政府应不断地寻找新的、合适的方法检测软件缺陷，以有效地降低软件供应链的风险。

而且，近年来，病毒等攻击事件越来越多，攻击技术也越来越复杂，政府部门应和私营

企业加强合作，灵活协调，以共同应对软件供应链中的新威胁、新挑战。

(1) 政府可与私营部门合作，成立一个以行业为主导的旨在解决软件产品保障问题的组织，类似 SAFECode。该组织以通过促进采用有效的软件保障方法，解决 ICT 产品流程中的安全问题为使命，尽可能寻找和推广最佳做法，开发和提供更安全、更可靠的软件和服务。

(2) 政府与私营部门合作，鉴别和加强关于软件保障的最佳做法，而不是试着去开发一个规定的方法，那么政府对于恶意代码插入的问题的回应更有可能成功。在大部分的高科技行业里，规范的做法通常是基于一定标准的，用一系列的评估程序来得到信任。

目前，有不少研究机构认为更健全的保障程序是，将私营部门驱动的最佳做法和现有的产品审查(例如，通用标准)相结合，即让行业来提出方案规则，让政府来实施他们，可以将认证程序与收购程序结合起来，这样可以加强通用标准的认证。政府可以通过设定收购的要求来领导软件行业，而不需要详细规定公司该如何开发软件。在这个收购驱动的方案中，会有一些较低敏感的应用的案例，这些公司可以自己认证他们已经遵循了最好的软件安全尝试。但是在其他情况下，一些外部的复审对于内部的认证来说是很有必要的补充[JAL2007]。

总之，将行业和政府的程序结合起来，形成一个新的管理模式，以适应在软件行业正在发展的生产模式。

5. 公司可采取的措施

公司作为软件开发的最重要的实施者，其安全性不言而喻。最佳方法是，综合在软件行业领先公司的软件安全策略，并加以整合利用。与其他软件公司的最佳实践一起参与分享，实现更好的软件安全，及时更新对于软件的要求和保障程序。但是，这一方法实施较难。

(1) 建立尽职检查表。公司为完善软件开发最佳方法建立“尽职”检查清单，从而加强认证步骤和帮助为信任代码提供保障。尽职检查表会要求开发者和编写者在编写安全代码上受到培训；公司在减低内部员工或者承包商的潜在的“内部威胁”风险上采取步骤；保证知识管理程序和在软件编写过程中跟踪软件代码的增添和更改的项目的存在；帮助代码编写和测试的风险建模；一个被独立的安全团队，包括在完成之后软件保障工具的使用，和外部承包商进行的渗透测试的对软件进行的正式复审[JAL2007]。

(2) 控制身份和访问管理。对于软件供应商来说，管理代码访问对确保其知识产权的安全性至关重要。公司可通过使用策略、过程和技术来管理员工对其知识产权的访问权限，从而降低供应链对其产品和服务产生的风险。公司可发放用于进行身份验证和访问控制的物理和数字凭证。员工根据业务需要结合使用这些凭证来访问公司的物理和电子资产(如源码管理系统)，从而提高针对某些电子资产操作的可说明性和可跟踪性。

(3) 加强防伪措施。公司应积极识别其软件的盗版版本，以确保用户不会面临盗版软件风险。并为减少盗版，公司应积极与全球执法机构合作，并使用策略、技术和过程来保持软件产品的完整性，包括代码签名和恶意软件检查。代码签名是指软件开发商能对其软件代码进行的数字签名。公司可规定在向公众发布文件之前，必须确保这些文件带有数字签名，从而有助于用户验证他们收到的软件是否来自该公司且未被篡改。同时，在

发布之前，公司可要求对产品进行扫描，以检查是否包含病毒和恶意代码。公司还可用源码管理、产品内部版本号和打包管理等流程来保持其产品的完整性。而且，公司还可提供教育、工程设计工具和强制策略，以帮助用户和组织识别盗版软件。

此外，公司应积极参加供应链安全讨论会，并积极采取措施以应对软件供应链中的各种风险。

6. 科研机构

首先，学术界应扩大软件供应链安全知识的普及，例如，将开发安全软件的重要性上升到大学课程的高度。其次，增加科研投资。毕竟让一个软件程序来测试另一个软件程序不是一个万能药。最新一代的软件工具，只是一个更大的保障工作中的一部分。软件工程变得越来越大，因此，在研究和开发更好的工具上的投资，对于很多软件产品的上百万条代码的初步检测，变得越来越重要。在开发更好的保障软件上研究和其他在信息保障上研究驱动的活动，对于降低供应链风险至关重要[JAL2007]。此外，国家可资助科研机构制作软件保障采购管理指导书，旨在帮助政府程序管理人员和合同签订人员在制作定制代码开发和商用现货软件采购及集成招标书的过程中囊括软件保障需求。

参考文献

[BF1999] Barbara Farbey & Anthony Finkelstein. Exploiting software supply chain business architecture a research agenda. 21st International Conference on Software Engineering, 16-22 May 1999. http://eprints. ucl. ac. uk/846/.

[BDW2008] Bart De Win, Riccardo Scandariato, Koen Buyens, Johan Gre goire, and Wouter Joosen. On the secure software development process CLASP, SDL and Touchpoints compared. Information and Software Technology, 2008.

[CJA2011] Christopher J. Alberts, Audrey J. Dorofee, Rita Creel, Robert J. Ellison and Carol Woody. A Systemic Approach for Assessing Software Supply-Chain Risk. 2011 44th Hawaii International Conference on System Sciences (HICSS), 4-7 Jan. 2011: pp 1-8.

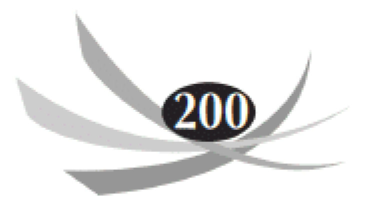
[CNSS2006] Committee on National Security Systems, National Information Assurance(IA) Glossary. CNSS Instruction No. 4009, 26 April 2010. http://www. ncix. gov/publications/policy/docs/CNSSI_4009. pdf.

[DACS2007] Information Assurance Technology Analysis Center (IATAC). Data and Analysis Center for Software (DACS), SOAR on Software Security Assurance, July 31, 2007. http://iac. dtic. mil/csiac/download/security. pdf.

[DHS2007] Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development. National Cyber Security Division, United States Department of Homeland Security. October 2007.

[DHS2009] Department of Homeland Security, Software Assurance in Acquisition and Contract Language. Software Assurance Pocket Guide Series: Acquisition & Outsourcing, Volume I, Version 1. 1, July 31, 2009.

[DSB1999] Defense Science Board. Final Report of the Defense Science Board Task Force on Globalization and Security. December 1999.



[DSB2007] Office of the Under Secret array of Defense For Acquisition, Technology, and Logistics. Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software, September 2007.

[DR2010] Dr. Robert, J. Ellison and Dr. Carol Woody. Considering Software Supply Chain Risks, Build Security In, 2010. https://buildsecurityin.us-cert.gov/resources/crosstalk-series/considering-software-supply-chain-risks.

[EF2007] Elaine Fedchak, Thomas McGibbon and Robert Vienneau. Software Project Management for Software Assurance. A DACS State of the Art Report, DACS Report Number 347617, 30 September 2007.

[FBX2009] 方滨兴. 软件确保. 中国计算机学会通讯, Vol. 5, Issue 1, 2009.

[FLL2009] 方滨兴,陆天波,李超. 软件确保研究进展. 通信学报, Vol. 30, No. 2. 2009.

[GMG2006] Gary McGraw. Software Security: Building Security in. Addison-Wesley Professional, February 2006.

[HH2008] Herman Hartmann and Tim Trew. Using Feature diagrams with Context Variability to model Multiple Product Lines for Software Supply Chains. 12th International Software Product Line Conference, 8-12 Sept. 2008: pp 12-21.

[JAL2007] James A. Lewis. Foreign influence on software risks and recourse. The Center for Strategic and International Studies (CSIS) Report, March 2007.

[JJ2006] Joe Jarzombek. Considerations in Advancing the National Strategy to Secure Cyberspace. December 2006. http://sysa.omg.org/docs/swa_washington_2006/US_Gov_SwA_Strategy.pdf.

[LF2001] Lynne F. Baxter and John E. L. Simmons. The Software Supply Chain for Manufactured Products: Reassessing Partnership Sourcing. Portland International Conference on Management of Engineering and Technology, Vol. 1, 2001.

[MLP2007] Mary Linda Polydys and Stan Wisseman. Software Assurance (SwA) in Acquisition: Mitigating Risks to the Enterprise, Draft Version 1.0, September 10, 2007.

[MSF1978] Marilyn S. Fujii. A comparison of software assurance methods. Proceedings of the software quality assurance workshop on Functional and performance issues, New York, USA, 1978: pp 27-32.

[MC2006] Mabel C. Chou and A. Ruchika. An In-depth Study of the Software Supply Chain. 2006 IEEE International Conference on Industrial Informatics, Singapore, 16-18 Aug. 2006: pp 753-758.

[MKKB2005] Mitchell Komaroff and Kristen Baldwin. DoD Software Assurance Initiative, DoD, 2005. http://proceedings.ndia.org/5871/Komaroff_Baldwin.pdf.

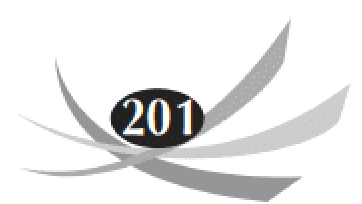
[NASA1989] National Aeronautics and Space Administration (NASA). Software Assurance Guidebook, NASA-GB-A201, September 1989. http://satc.gsfc.nasa.gov/assure/assurepage.html.

[NASA1992] National Aeronautics and Space Administration (NASA). Software Assurance Standard. Standard No. NASA-STD-2201-93, November 10, 1992.

[NASA2004] National Aeronautics and Space Administration. software assurance standard, NASA-STD-8739.8 w/Change 1, July 28, 2004. http://www.hq.nasa.gov/office/codeq/doctree/87398.pdf.

[NIST] NIST. SAMATE-Software Assurance Metrics And Tool Evaluation. http://samate.nist.gov/Main_Page.html.

[OWASP] OWASP. Software Assurance Maturity Model. http://www.opensamm.org/.



[PWC2011] PWC. Transportation &Logistics 2030 Volume 4: Securing the supply chain, 2011. https://www.pwc.com/en_GX/gx/transportation-logistics/pdf/TL2030_vol.4_web.pdf.

[RAM2006] Robert A. Martin. Software Assurance Programs Overview, December 2006. http://sysa.omg.org/docs/swa_washington_2006/SwA_Programs_Ovrvw.pdf.

[RO2007] Roy Oberhauser, Rainer Schmidt. Improving the Integration of the Software Supply Chain via the Semantic Web. International Conference on Software Engineering Advances (ICSEA 2007), 25-31 Aug. 2007.

[RJE2010] Robert J. Ellison, Christopher Alberts, Rita Creel, Audrey Dorofee and Carol Woody. Software Supply Chain Risk Management: From Products to Systems of Systems. CMU/SEI-2010-TN-026, December 2010.

[RJEJBG2010] Robert J. Ellison, John B. Goodenough, Charles B. Weinstock and Carol Woody. Evaluating and Mitigating Software Supply Chain Security Risks. CMU/SEI-2010-TN-016, May 2010.

[SAF2007] DHS Software Assurance Forum Measurement Working Group. Practical Measurement Guidance for Software Assurance and Information Security, DRAFT, Version 2.0, Mar 3, 2007.

[SAFECode2010] SAFECode. Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain. SAFECode, June 14, 2010.

[SJ2006] Slinger Jansen, Sjaak Brinkkemper, Gerco Ballintijn and Arco van Nieuwland. Integrated Development and Maintenance of Software Products to Support Efficient Updating of Customer Configurations: A Case Study in Mass Market ERP Software. Proceedings of the 21st IEEE International Conference on Software Maintenance, 26-29 Sept. 2005: pp 253-262.

[STR2006] Samuel T. Redwine, Baldwin R O, Polydys M L, et al. Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software, draft version, 2006.

[DHS2003] Department of Homeland Security. National strategy to secure cyberspace. February 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

[Microsoft] Microsoft. http://www.microsoft.com/security/sdl/default.aspx.

[DG2006] Dan Graham. Introduction to the CLASP Process. November 16, 2006. https://buildsecurityin.us-cert.gov/articles/best-practices/requirements-engineering/introduction-to-the-clasp-process.

[DHS] Department of Homeland Security. What is Build Security In? https://buildsecurityin.us-cert.gov/.

第8章 ICT 采办安全

8.1 概　　述

在20世纪90年代末期,美国已经意识到采办问题的严重性。1998年5月22日,克林顿发布的第63号总统令里面就已经提到,应当确定大型采办任务中与其相关的信息安全。其中提出:在联邦机构的采办过程中,要反映出信息保障的重要性,并且在必要的时候,拿出有关的建议,对整体的采办过程进行检查和修改,这样才有利于信息安全的保护。在布什执政期间,这个问题被进一步明确了。2002年,布什开始起草国家安全战略,进一步提到了采办的步骤和过程,以及相关的标准。

在布什政府执政后期,随着全球信息安全形势日益严峻,ICT供应链安全问题开始进入政府的视野。2006年4月,美国国家科技委员会发布了《联邦网络安全和信息保障研发计划》,明确将ICT硬件和软件的供应链攻击视为一种攻击趋势,并认为这种安全问题仅靠严格的检测是无法解决的。但是,在该计划中仅将供应链攻击视为一种特殊的"内部人员攻击"。

2008年12月,在奥巴马上台之前,美国智库战略与国际研究中心(CSIS)发布了《在第44任总统任期内保护网络空间安全》的咨询报告,向新总统提出了若干重要建议。其中便包括"通过采办规则提高安全性",希望政府能与工业界合作,共同制定和执行ICT产品(其中软件居首要位置)采办安全指南。

奥巴马政府执政后,进一步重视信息安全问题,将信息安全视为最严峻的经济和国家安全挑战之一。2009年5月,奥巴马政府发布了对美国网络空间安全政策的评估报告,并根据评估结果开展了新一轮的动作。这个评估报告继承了国家网络安全综合计划(CNCI)对ICT供应链问题的判断,并将其作为国家信息安全威胁的一种,重申了采取综合、体系化对策的重要性。从其措辞不难发现,美国已经完全将ICT供应链安全问题与"国外"机构相提并论。奥巴马政府在报告中同时指出,仅仅谴责国外产品和服务供应商是不够的,新的供应链风险管理方法势在必行。由此可见,ICT供应链采办安全是十分重要的。

目前,国防采办流程在生产武器上耗时过长,这些武器成本昂贵,应用于战场时通常在技术方面已经过时。典型的主要系统采办需要花费10～15年,然而在商界中,复杂程度与其类似的新系统开发仅需上述时间的三分之一到二分之一。很多国防系统紧密依赖的信息技术的采办同样超出典型商业开发时间——所需时间是其三至四倍。技术的快速进步远远超过这些开发时间,这意味着当一个系统被提供至战士使用、用于战场时,子系

统技术已落后了一或两代——除非在系统投入使用前已进行升级。此外,国防项目通常伴随着成本大幅超支、进度长期延误以及产品质量和性能不符合要求等问题。

相比于国防采办流程,企业采办在安全性上面的要求较低。通过建立业务分析,对有价值的信息数据进行业务分析后,能够实现对物料采办执行过程的动态监控,实现对已完成采办业务的绩效评估;通过业务数据分析能不断实现组织机构的优化和重组,实现企业采办过程的持续绩效改进。依据准确、有效的数据统计可以得出极具价值的分析结果,从而提供对采办决策的支持。例如:采办成本降低分析、采办成本差异分析、采办价格与采办比例对照分析等。建立信息预警体系,实现实时监控也十分重要。通过信息自动预警系统和业务分析系统能够针对物资计划、采办、存货等环节过程中的主动警示和已完成业务的分析,使管理人员能够掌控业务执行人员的工作效率,有效督促考核业务的执行情况。

公开、透明、科学的采办流程,使事后审查变为事前监督,对采办过程做到有据可查,有据可依。采办方企业通过信息化采购交易平台的专业数据库的帮助,可以跳出地域、行业的限制,找到更多、更合适的供应商。这将进一步丰富采办方企业的供应商资源和情报,使其深入了解相关物资和产品的市场供求情况。在此基础上,可以根据供应商的资信,整合供应商资源,这些都使市场供求关系更加明了。

网络信息化建设可以为采购管理带来质的飞跃。事实上,利用信息化来不断深化管理,不断提高业务管理能力和专业化能力、提高公司的核心竞争力已经成为所有人坚定不移的共识。不过如何建立高度集成、高效协作、快速响应的安全采办运行体系仍是业内探讨的重点。

8.2　ICT 采办基础

实施 ICT 供应链管理的目的是利用信息网络技术整合企业内外资源,使之以较低成本为项目提供满足要求的服务、中间产品和制成品,提高资源利用率实现效益增长。采办是 ICT 供应链管理中非常重要的环节,据统计,ICT 企业要用销售额的很大比例来进行原材料、零部件、设备的采办,因此对采办环节的控制是项目管理的关键。

8.2.1　ICT 采办机制

ICT 采办机制可分为如下四个阶段。

第一阶段,确定 ICT 产品或服务的需求。在采办部门负责的组织和控制下,制订 ICT 采办战略,制订策略性需求,对 ICT 产品和服务采办需求进行评估和认证。

对于制定一个好的 ICT 战略,关键是了解近年来的 ICT 配件运行的如何,以及它们对企业的影响。因此采办部门首先要做的事情就是对近年来的情况进行调研。要了解目前的 ICT 配件的状况,需要考虑多方面的因素,具体表现在 ICT 配件是否得到了充分的利用,是否能够满足现阶段需要以及用户是否满意。这就要求采办部门收集多方信息,包括用户的反馈信息,企业资金的 ICT 团队、经理,伙伴和消费者。

在对目前的 ICT 配件状况有了一定的了解之后,还需要计算安装 ICT 配件的成本。

提前做好预算是十分有必要的一步，因为这样就可以比较计划开支情况和实际开支情况之间的差距。当实际花费超过预算时，采办部门要清楚是因为什么原因造成的，尤其是当采办了全部计划配件而这个配置的表现却达不到预期期望时，就不得不深究一些，弄清楚造成这个资金缺口的原因。

当将所有这些信息收集齐全后，下一步需要分析的是在过去的一年中ICT基础架构遇到的问题，这很容易通过访问ICT日志记录数据分析后完成。通过访问ICT日志记录数据，可查明导致大多数问题的独特事件，以及由它造成的损失有多大，范围有多广。而需要格外进行调查的是这些事件导致多少用户受到影响，完全解决这个问题需要多长时间，对企业的全面影响是什么，以及今后防止这种袭击应做什么，一旦找到了影响企业ICT配件的关键问题及其背后的原因，就会知道在下一阶段的采办清单中什么是应该优先考虑的。

一旦大概了解了主要事件以及对工作的影响，需要做的下一件事就是进行ICT咨询，通过询问经理和ICT团队的意见，找出解决问题的办法。在得到建议的解决方案后，就可以进行可行性研究。

有了这些基础之后，再决定要采办什么ICT产品，就有了一个起点。在这个阶段，可以根据它们对工作的影响开始筛选，最终会得到一个经过筛选的需要采办的项目清单。可以把它们分类地收集在一起，制定一个需求时间表，在这个表里，明确指出哪些ICT产品是需要立即采办的，哪些ICT产品虽有必要采办却并不急需，可以等到下一个采办周期再进行采办的。当这样一个分类采办清单确定之后，就可以开始制作每个项目的说明了。

第二阶段，是ICT供应商的资格认证。在这个阶段需要评价和选择ICT供应商，并对ICT产品的采办价格进行初步评判，此过程由ICT采办中心负责组织和控制。

对于确定销售商的问题，可以从相关渠道找到销售商的信息，比如说可以通过查询合适的销售商，通过访问其主页，在销售商的网站上核查其提供的产品和说明，与之前确定的采办清单相对比，很好地了解市场上供应什么，与之前预估的价格是否有大的出入，找到适合采购的需要的销售商。

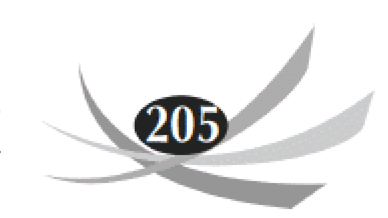
下一步让各种各样的销售商报价，开始谈判争取最佳协议。在选择销售商时，选择那些可以根据你的采办清单提供多种产品的销售商是明智的，因为这使ICT基础设施更标准完善。在信息主管的期望与销售商的最终供货之间总是存在差距的，为避免这种情况，应该在签约之前测试某些设备，而且要与销售商有严格的服务登记协议。

第三阶段，是ICT采办项目的谈判、合同管理、下达采办订单和承诺的过程，此过程也由采办部负责组织和控制。

第四阶段，主要是ICT采办的事后评估，包括满足用户需求能力的评估、ICT供应商的表现分析、售后服务跟进、项目结束和订单终止等事项，由采办部门负责组织和控制。

8.2.2 ICT采办注意事项

面对让人眼花缭乱的促销宣传攻势，企业的ICT采办人员如何睁大慧眼，做出理性的选择呢？笔者认为，在经济环境不稳定的时候，企业采办应更趋于谨慎，每一分钱都要



花在刀刃上，同时希望能够真正从业务的支持中得到回报。

对于规模较小的企业，在ICT采办上自然也对价格比较敏感，倾向于选择低价位的电子产品来满足最基本的使用需求。殊不知，这些企业往往缺乏专门的ICT人员，如果一味追求低价而忽略了产品的性能，很可能会给日后的使用埋下隐患。所以，兼顾了低价和高品质的产品才应该是这类企业的首选。

在采办的过程中，更应注意如下问题。

(1) 错误的地点、错误的时间。对于中小型企业来说，采办的时机与地点是值得关注的问题，如果在恰当的时机开展采办活动，例如在某厂商进行产品促销时，将会减少采办成本。但是通常采办的时间与地点不会得到重视，从而被中小企业忽视。ICT产品的更新速度相对来说是很快的，随着产品的更新换代，势必伴随着老型号商品的降价，而这种降价并不是毫无章法随机而为的，根据市场调查，很容易发现，春夏两季是ICT厂商的促销旺季，新品上市、降价促销都是惯用手段，大型的卖场或者电脑城、专卖店、直销商都会有大量的促销活动。如果能把握住这个规律，确定ICT采办的黄金时间，对于人数不多的小企业采办而言，将会大大节约成本[XY2009]。

(2) 贪图价格便宜。中小企业在选购ICT设备的时候，更多会考虑到节约采办资金的问题，事实上，适当的购入高性能设备，才能获得最优性价比。对于那些所有工作都必须由计算机处理的事务，尤其是像图形处理等硬件要求较高的复杂任务，设备性能的任何一点提升都会大幅度提高工作效率。设备的高性能会大大缩短工时，从另一方面说，这就相对节约了成本，提高了生产效率。在这种情况下，为高性能付出更多的金钱就是值得的。因此，中小企业在采办ICT产品时，还应适当的从工作效率的角度来考虑，不能一味地贪图便宜[XY2009]。

(3) 盲目追求高端。同上一种情况截然相反的一种误区是，中小企业的普通ICT设备也盲目地追求高性能。这样不仅造成采办的浪费，还会造成耗电、管理、网络设备、多余的宽带、不必要的覆盖范围等等浪费现象，为此多付出金钱是不值得的。而且，很多情况下，中小企业并不具备专业的IT人才，往往是花了大价钱买来了高端的设备却并不能得到恰当的利用[XY2009]。

相比之下，大中型企业客户的ICT投资眼光更具“全局观”，尤其在TCO(总体拥有成本)的理念逐渐被企业用户所接受的今天，高质量ICT产品的稳定性能成为他们选择产品着重考虑的因素。大中型企业客户的电脑数量很多，聪明的ICT经理不得不考虑维护、数据安全、能耗等各方面的因素。而且随着电脑在企业中的普及，电脑设备出现故障不仅意味着耗费大量资金和时间，还可能影响到业务的正常运转，甚至是危及企业最核心的数据安全。当然在已经达到中等规模的企业当中，行业的特征也愈发显著，所以采办ICT硬件的时候开始倾向于关注整体的解决方案而不是单独的产品。对于大中型企业来说，在选购ICT设备的时候更应该着眼于全局，选择值得信赖的合作伙伴，以及能提供一定的行业增值服务的厂商。

8.2.3 ICT采办新趋势

对于一个企业来说，能有很多的技术和可行性方案供选择固然是件好事，但是，这无

形中也增加了企业选择的难度——因为企业要分析究竟谁的技术或者解决方案才是最合适于企业自身业务的。今天，企业的ICT基础架构已经比以前复杂了许多，这更加证明了对ICT采办重视的必要。实际上，ICT采办并不意味着仅仅只要一次性付钱，把设备或者软件买来装好就成，还需付钱购买相关的服务、维护、认证号码等。因此，需要强调的是ICT采办的过程实际已经远不只是产品的购买。随着市场上花样繁多的解决方案可供选择，CIO(Chief Information Officer，首席信息官)们也要为买什么和不买什么付出更多的心血，因为即使是一个错误的ICT采办也有可能导致巨大的损失甚至是一个项目的失败。

有一点是毋庸置疑的，现代市场竞争日益激烈，消费者的价值观、生活方式以及消费的需求层次、水平和结构也都在不断改变，所以企业业务差异化优势在竞争中显得尤其重要。其中，新型先进的信息技术是提升企业特有品牌和效率的关键。企业必须进行不断创新，在ICT采购方面运用合理的决策和方法，才能具备充足的技术条件，以对抗各种挑战，保持对市场的影响力和占有率。因此现代企业在ICT方面投入越来越多，有关ICT预算自然也随之逐年增长。BCP(Business Continuity Planning，业务连续性计划)、通信、信息安全以及整合服务等正在获得越来越多的重视。

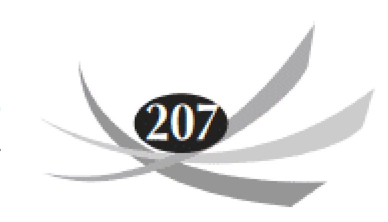
综合来讲，ICT采办正呈现如下趋势。

1. 采办信息渠道多种多样，便利与风险同在

在ICT比较发达的地区，当中小企业在采办信息化产品时，信息获取的主要渠道也变得五花八门。部分中小企业通过网络、展会、平面广告等来获取信息，也有ICT厂商主动上门自荐。目前互联网正逐渐成为中小企业获取ICT信息的主要渠道，他们大多是通过互联网查询自己所需要的产品，对产品进行充分了解、比较，判断是否满足自己的需求或是否适合自己使用，然后由单位统一进行采办。ICT产品的热销也导致了代理销售渠道五花八门，在为企业提供便利的同时，面对良莠不齐的购买渠道，也增加了采办过程的风险，因此企业应慎重选择[YK2009]。

门市购买快质量价格不透明。在网络通信技术发达、网商林立的今天，通过门市购买依旧是大多数企业采购负责人购买的主要渠道，因为在门市可以现场看货，且大多企业都是急买急用，而门市购买支持随时买随时提货。但门户购买也存在许多弊病，众多消费者反映在门店购买中遇到被“宰客”的情况。在门店购买过程中，尽量多压价格且向销售商索要原厂资质证明，且注意观察门市供应商是否有售后服务资质。

网上搜索货比三家、骚扰多、沟通难。通过网上搜索供应信息也成为越来越多企业采购负责人购买的渠道之一。网上信息量大，在网上搜索时可以非常方便地货比三家，看谁的价格更为合适，但透漏自身信息广，获得的骚扰也多，经常陷入面对和诸多供应商讨价还价的僵局，且看不到供应商的自身资质，无法了解他们售卖产品口碑和服务状况，在价格参考上确实非常方便，可以很快剔除价格离谱的，但沟通难，一些供应商专业资质匮乏无法深度交流，还常有骚扰电话，有些网络供应商在起初报出非常高价被拒绝后，不断的打电话过来降低价格以期达成交易，且价格适中的也会一起参与，经常被三五家的销售一起追踪，确实烦不胜烦，而且购买过程中还得格外小心，谨防买到仿制品。因此在网上搜索过程中，注意保持自己个人隐私信息不要泄露，此外也注意对产品正品性的一个考量。



合作采购商采购便捷成本过高。通过采购商采办是一些大中型企业的主要购买渠道。交办给供应商后，采购就省事很多，企业无需投入大量的精力。但也有一些死角，在采购过程中也无法避免，中间多了一道经手人成本必然会增高，此外在这个过程中，容易出现企业内部人员收受回扣出卖企业利益的情况。因此在采购过程中，要谨慎选择供应商和负责接洽的负责人，否则企业利益长期受到侵害[YK2009]。

网上商城直接订购价格适中信任难。通过网上商城的订购已成为大多企业考虑的主要购买渠道。通过在各大网上商城看货，价格比对一目了然，日益完善物流机制也解决了买后苦等的尴尬，且大型网上商城都有一个良好的口碑机制，购买的网友都会对商城售卖产品质量好坏和存在的一些问题做出评点，在购买时可以直接参考商品页下信息作出判断，但网上商城售卖也仍存在一些问题，首先采购者难以对网站产生信任，其次大多网上商城售后服务不便。

2. 更多倾向于全价值链解决方案

中小企业普遍存在对信息技术认识不足、专业人才缺乏、网络应用匮乏以及信息实施过程繁杂等特点，因此，为了更好地适应信息化的冲击和市场挑战，中小企业将不再满足于厂商提供的单一产品和技术，而是渴望得到高性价比的整体解决方案。在与 ICT 厂商的合作程度上，更趋向于各个环节环环相扣。这就要求 ICT 厂商与企业建立区别于传统方式的新型合作方案，从最基本的“设备供应”的方式逐渐转变为提供“基于 ICT 的全面服务”这样一来，厂商在提供实用易用、高性价比产品的同时，也要提供完整良好的售后服务和咨询培训。甚至为不同的客户量身打造个性化的解决方案[YK2009]。

3. “傻瓜产品”受青睐

产品是否具备“简单、易用、快捷”等特点是企业信息化建设和 ICT 采办的关注点。中小企业其实并不需要配备结构复杂、使用烦琐的 IT 产品，初次采办成本低廉、性能稳定、易用通用、容易维护的 ICT 产品才是它们最为需要的。通俗来讲，就是要把 ICT 产品做成“傻瓜式”，争取一键搞定。尤其是当面对关键客户——企业的决策者时，管理者日常事务繁多，没有多余的时间面对软件中满屏的选项进行操作，如果不能迅速找到他想要看的东西，他们会觉得烦琐，从而拒绝使用。因此，给决策者服务的软件越简单越好[YK2009]。

8.2.4 与传统采办模式比较

传统项目采办的重点放在与供应商进行商业交易的活动上，通过供应商的多头竞争，从中选择价格最低的作为合作者。质量、交货期也是采办过程中的重要参考因素，但在传统的采办方式下，质量、交货期等都是通过事后把关的方式进行控制的，如货到验收等。传统采办的交易过程将重点放在价格的谈判上，因此在供应商与采办部门之间经常要进行报价、询价、还价等来回的谈判，并且多头进行，最后从多个供应商中选择一个价格最低的供应商签订合同(如表 8-1 所示)。

而供应链管理下的采办模式是一种订单驱动的采办方式，它与企业的采办方式和传统的采办方式有所不同，这些差异主要体现如下。

(1) 一般买卖关系向长期合作伙伴关系甚至到战略协作伙伴关系的转变。在传统的

采办模式中，与供应商的关系通常是短期的买卖关系，采办理念停留在压榨供应商以最大程度的节约成本上，这必然将导致供应商的频繁更换，无法保持长期的合作。在供应链模式下，与供应商的关系已经转变为长期合作伙伴关系甚至是影响企业未来发展的战略协作伙伴关系，企业与供应商之间签订供应合同的手续将大大简化，不再需要双方的询价、报价的反复协商，大大降低了交易成本。企业与供应商之间共享库存和需求信息，共同抵御市场风险，共同研究制定降低成本的策略，把相互合作和双赢关系提高到全局性、战略性的高度[YXG2008]。

表 8-1 采办对比

项 目	供应链环境下的采办	传 统 采 办
采办批量	小批量，送货频率高	大批量，送货频率低
双方关系	长期合作，战略协作	短期合作，多为竞争
供应商评价	强调价格	多标准并行考虑
质量检查	买房参与，实时控制	事后把关
协商内容	共同控制成本、质量	获得最低价格
信息交流	快速、可靠、信息共享	一般要求，信息专有

(2) 从内部资源管理向外部资源管理转变。在传统的采办模式中，采购注重对内部资源的管理，追求采购流程的优化、采购环节的监控和与供应商的谈判技巧，缺乏与供应商之间的合作。在供应链管理模式下，转向对外部资源及对供应商和市场的管理，增加了与供应商的信息沟通和市场的分析，加强了与供应商在产品设计、产品质量控制等方面的合作，实现了同步化供应链协调，生产、供应计划能够并行进行，缩短了用户响应时间，实现了供应链的同步化运作[YXG2008]。

(3) 信息传递方式发生了变化。在传统采办方式中，供应商、分包商对施工生产过程的信息不了解，也无需关心总承包企业的生产活动。但在供应链管理环境下，供应商能够共享总承包企业的信息，提高了供应商的应变能力，减少了信息失真[YXG2008]。

(4) 实现了面向过程的作业管理模式的转变。在传统的采办模式中，采办的目的就是为了补充库存，即为库存而采办，采办过程缺乏主动性，采办计划较难适应需求的变化。在供应链管理模式下，采购活动紧紧围绕用户需求而发出订单，因而不仅可及时满足用户需求，而且可减少采购费用，降低采购成本。订单驱动采办方式简化了采办的工作流程，采办部门的作用主要是沟通供应商与生产部门的联系，协调供应与生产的关系，为实现精细采办提供了基础保障[YXG2008]。

(5) 确保工程承包商能致力于其核心业务。工期内的所有工程进展、用料安排和施工计划都通过数字系统传送给供应商，由供应商确定材料运送时间、种类和数量。供应商还可以通过数字系统、视频会议系统以及 EDI 等方式及时撤回剩余用料、更换不合格材料、补充急需材料，同时向工程承包商推荐先进、经济和新兴材料。因此工程承包商不需或很少需要材料库存设施，这也是一种对成本的节约[YXG2008]。

8.3 ICT采办安全

8.3.1 ICT采办风险分类

1. 人为风险

人为风险人是信息安全最主要的风险因素。不适当的信息系统授权，会导致未经授权的人获取不适当的信息；采办人员操作失误或疏忽会导致信息系统的错误动作或产生垃圾信息；违规篡改数据、修改系统时间、修改系统配置、违规导入或删除信息系统的数据，都可能导致各种重大采办事故的发生。有令不行、有禁不止等人为因素形成的风险，是严重的信息安全风险，尤其对军队来说，是物资采办信息安全的最大风险。企业应根据物资采购各个不同过程，建立各个环节的续效考核制度，把采购任务和各项相关指标和责任转化分解，明确规定出库存指标和工作标准，分解，落实到各有关部门和个人，结合经济效益进行考核，层层把关，调动积极性。以尽量避免采购风险的发生。

2. 系统风险

系统风险包括系统开发风险和系统运行风险。在采办项目开发过程中没有考虑到必要的信息系统安全设计，或安全设计存在缺陷，都会导致采办信息系统安全免疫能力不足。没有完善、严格的生产系统运行管理体制，会导致机房管理、口令管理、授权管理、用户管理、服务器管理、网络管理、备份管理、病毒管理等方面出现问题，轻则产生垃圾信息，重则发生系统中断或信息被非法获取等问题。

当前的采办信息系统已是一个庞大的网络化系统，在网络内存在众多的中小型机、服务器、前置机、路由器、终端设备，也包括数据库、操作系统、中间件、应用系统等软件系统。网络系统中的任何一个环节都有可能出现故障，一旦出现故障便有可能造成系统中断，影响业务正常运作。同时，由于自然灾害、战争等突发事件造成的系统崩溃、数据载体不可修复性损失等等，都会给采办信息系统带来很大的影响。

3. 数据风险

数据是信息的载体，而对于物资采办来说，数据是系统重要的资产。对数据的存储、处理、获取、发布和共享均需要有一套完整的流程和审批制度，没有健全的数据管理制度，将存在导致数据信息泄露的风险。针对核心的敏感数据区，更是要采取一系列措施保证数据的安全。根据关注的数据风险差异，应用场景的不同而提供多元化的解决方案，在方案中所有体系既独立，又可以互相组合形成更完整的解决方案，同时也能够提供优良的扩展性，是企业能够基于不同应用的数据采取不同的保密解决方案。

8.3.2 ICT采办信息安全三要素

信息安全的含义在不同的环境情况下各不相同。提起信息安全，人们最容易想到的就是计算机的病毒问题。不错，如今互联网成了感染病毒和间谍软件的最主要的媒介。但是，信息安全不单是防毒查毒的问题。在国际标准ISO 17799信息安全标准中，信息安全是指：使信息避免一系列威胁，保障商务的连续性，尽量减少业务损失，从而最大限度

地获取投资和商务的回报。

信息系统存在着脆弱性，也就是技术上的漏洞，这些漏洞，脆弱性再加上人为或自然的威胁，使得一些信息安全事件的发生存在可能性且这些事件将造成影响，多数为负面影响。也就是说脆弱性和威胁是原因，可能性和影响是结果，当然还有一些其他的要素。对于ICT采办系统，信息安全管理则应该坚持系统和全局的观念，基于立足应急保障的思想来建立起安全管理体系。通过系统、全面、科学的安全风险评估，体现“积极预防、综合防范”的方针，强调遵守国家有关信息安全的法律法规及其他合同方要求，透过全过程和动态控制，本着控制费用与风险平衡的原则，合理选择安全控制方式，保护关键信息资产，使信息风险的发生概率降低到可接受的水平，确保信息的保密性、完整性和可用性，保持组织业务运作的持续性[ISO/IEC17799]。

1. 信息安全的保密性

对保密性而言，信息不能泄露给未授权者，这些未授权者可能包括个人、实体或者是过程。泄露的途径有很多，例如口头泄露、通过网络、打印机、复印机、USB存储设备等都有可能泄露。我们可以这样通俗的理解保密性：只有被授权的个人、实体或者是过程才能访问受保护的信息。保密性是在日常的信息安全工作中强调的比较多的方面，也是我们最容易理解的一个属性。ICT采办系统要求在确保遵守保密守则规定的前提下，确保涉密信息仅可让授权获取的相关人员访问。结合当前的状况，ICT采办系统的信息安全保密应当做到：严格分岗授权制衡机制，杜绝不相容岗位兼岗现象；严格用户管理和授权管理，防止非法用户、用户冗余和用户授权不当；加强密码管理，防止不设口令或者口令过于简单；加强病毒防范管理，防范病毒损害；控制访问信息，阻止非法访问信息系统；确保对外网络服务得到保护，阻止非法访问网络；检测非法行为，防范道德风险；保证在使用移动电脑和远程网络设备时的信息安全，防止非法攻击。

2. 信息安全的完备性

完整性通常被理解为“防止未授权的更改”和“防篡改”等，在不同的环境往往被赋予不同的含义。在信息安全领域，信息资产的完整性往往还要意味着：准确而且正确的、未篡改的、仅能以被认可的方法更改、仅能被授权人员或过程更改、有意义且能用的。在ICT采办时，具体要求是：严格采办业务流程管理，确保采办业务流程与采办信息系统操作流程完整一致；严格控制生产系统数据修改，防止数据丢失。防止不正确修改，减少误操作；严格数据管理，确保数据得到完整积累与保全，使系统数据能够真实、完整地反映采办业务信息；严格按照企业关于物资采办的规定和要求操作，减少或杜绝非招标业务；避免任何违反法令、法规、合同约定及易导致业务信息与数据信息不一致、不完整的行为。

3. 信息安全的可用性

可用性通俗地讲就是“合法用户想用时能用”。一个目标或者服务被认为是可用的，应该：以能用的方式呈现、有满足服务要求的能力、有清晰的流程，如果在等待状态下，这种等待不是无限期的、服务在可接受的时间段内可以完成。具体到ICT采办，要确保被授权人可以获取所需信息。具体要求是：加强生产系统运行管理，确保生产系统安全、稳定、可靠运行；加强生产机房建设与管理，保障机房工作环境所必需的湿度、温度、电源、防火、防水、防静电、防雷、限制进入等要求；加强生产系统日常检查管理，及早发现故障苗

头；加强系统备份，防止数据损失；严格生产系统时间管理，禁止随意修改生产系统时间；保障系统持续运行；实施灾难备份，防止关键业务处理在灾难发生时受到影响。影响信息完整性的因素常见有：信息的来源，涉及到从哪里获得、如何获得、通过谁获得；信息到达前受保护的状况；信息在抵达本组织后受保护的情况等。

8.3.3 ICT采办管理特征

1. 变被动采办为主动采办

传统采办中，采办部门的职能和权限相对集中在采购上，无法参与到整个采办程序。其中需求是由需求管理部门提出的，供应商也是由各需求管理部门进行推荐的，对市场的调查和产品的测试工作也都是需求部门和需求管理部门独自完成的，这些过程，采办部门都没有参与，因此采办部门无法进入供应链的前端，无法在第一时间了解供应商、市场和产品的情况。

在ICT供应链管理模式下的采办则解决了这个为题。ICT采办要求各采办部门在采办项目启动前就进入“角色”，连同需求部门一同进行采办产品的市场调查、潜在供应商选取和产品测试等相关活动。如此一来，采办部门能对供应商进行实地考察并进行技术测试，掌握供应商及其商品的信息，做到好中选优，达到“优质采办”和“主动采办”的工作目标。采办人员在了解供应商、市场和产品等详细情况后，再进行商务谈判阶段就有的放矢，不至于非常被动，采办就不会成为仅仅是进行“讨价还价”的工作，从而提高了采办谈判的效果和效率。

2. 从一般买卖关系转变为战略合作伙伴关系

一般情况下，采办主要涉及三方面的参与者：采办需求部门、采办部门和供应商。基于传统的采办模式中，采办部门与供应商之间只是简单的买卖关系，这种合作是短期的，企业与供应商通常只会从自身利益出发，做出考虑。而在ICT供应链管理模式下，供应与需求之间的关系，已由买卖关系转变为战略伙伴关系。企业对ICT供应商必须有全新认识，应该把供应商当作伙伴，把自己当作供应商与用户间的桥梁。各个参与者之间的合作通常是趋于长期的、战略性的。因此企业与供应商之间的联系十分紧密，他们共同研究企业整体市场的内在规律，制定满足企业生产需求最有利、最快捷、最安全的服务方式，共同承担着整个供应链价值创造的责任，任何一个环节出现问题，都将对整个供应链产生巨大的影响。只有最大限度地减少审批环节、简化送货流程、规范结算程序、提高各环节办事效率、净化采购环境、降低供应商的交易成本，才能赢得供应商的真诚合作。

对于一些涉及全局性、战略性的供应链问题，战略伙伴关系的采办方式更是解决这些问题的必要条件。这种关系的收益是多方面的，供需双方通过战略性合作关系，可以降低由于不可预测的需求变化带来的风险；可以为双方共同解决问题提供便利的条件，双方可以为制定战略性的采办供应计划共同协商，不必为日常琐事消耗时间与精力；供需双方都从降低交易成本中获得好处，避免了许多不必要的手续和讨价还价的过程；信息的共享避免了信息不对称、决策可能造成的成本损失，消除了供应过程的组织障碍，为实现及时化、准时化和精确化采办创造了条件。

3. 从局部采办到全流程采办

传统采办将重点放在了采办价格谈判环节，而忽视了对采办其他流程的管理。ICT供应链管理模式下的采办，要求对全流程进行管理，其中包括供应商管理、评标委员管理、采办商务谈判、评审管理、合同执行情况管理、售后服务管理等，这就要求企业在采办工作中做出相应的改变，需要重新修改规章制度，补充采办类型的人才。更重要的一点是，全流程采办实现了采办的过程完整化，不再只是局于形式，而是实实在在的采办工作。

8.3.4 ICT立法保证

1. 国家安全系统领域对ICT产品的采办要求

美国的国家安全系统是指对于国家安全至关重要的信息系统，NIST SP 800-59《将信息系统标识为国家安全系统的指南》对如何确定国家安全系统提出了明确规定。早在2001年，美国国家安全电信和信息系统安全委员会便宣布，自2002年7月起，在国家安全系统中强制使用经过美国NIAP(国家信息保障联盟)认证的ICT产品。虽然美国已与其余20多个国家共同签署了信息技术安全通用评估准则(CC)的互认协定，但其国家安全系统的采办清单上迄今没有出现过由他国信息安全认证机构认证的信息技术产品[NIST SP 800-59 2003]。

2. 在联邦信息系统安全指南中提出的安全控制要求

美国国家标准与技术研究院(NIST)在发布800-53《对联邦信息系统和组织的安全控制建议》时，将“系统和服务采办”列为一项重要的信息安全控制类，该控制类的第12项要求便是“供应链保护”，其安全控制措施要求联邦政府机构对供应链风险进行防范，在系统安全生命周期范围内关注脆弱性。可选的增强措施包括：在采办系统软硬件和服务前就要对服务提供商进行细致审查和选择，建立可信的交付渠道，在同一系统中要采办多个供应商的产品，缩短采办决定交货的时间差，必要时对系统进行渗透性测试。根据《联邦信息安全管理法案》，NIST发布的800-53对所有的联邦机构都具有强制性作用[NIST SP 800-53 2009]。

3. 立法中对联邦政府采办制度的改革要求

2010年3月24日，美国参议院商务、科学和运输委员会全票通过了由参议员杰伊·洛克菲勒和斯诺·盖恩提交的《网络安全法案》，目前该法案将进入参议院全院表决程序。这是美国历史上一部很少见的综合性的信息安全立法议案。议案高度关注联邦政府的ICT供应链安全，为联邦政府采办ICT产品提出了法律条款。根据该立法议案的规定，采办工作的责任部门是总务管理局，实施途径是由总务管理局制定统一的信息要求书(RFI)和建议要求书(RFP)格式，在其中明确对ICT产品和服务的安全要求，任何联邦机构不得违背。

8.4 美国国防部采办安全

信息技术作为现代武器系统的关键要素，它的快速发展给采办管理工作提出了新的要求。美军在信息技术采办工作中经过多年的实践，形成了完善的管理体系，改进了采办



程序,在人才队伍建设方面也积累了丰富的经验。但是也同样存在着采办职责划分不合理、采办程序不能适应信息技术特点,以及采办人员经验不足等问题。

8.4.1 美国国防部ICT采办管理

在1958年以前,美国武器装备采办由三军分别管理,各军种设有完备的装备采办管理机构,军种间互不通气,造成重复浪费和各行其是的现象。为克服分散管理造成的弊端,美国国防部采办实行国防部统一领导与军种分散实施相结合的管理模式。所谓统一领导,是指在国防部专门设置了采办、技术与后勤副国防部长一职,统管全军信息技术研发及采办事务。而分散实施,是按信息技术项目的重要性及费用多少,实行分类、分级管理。对于不同类别的信息技术采办项目,负责采办、技术和后勤的副部长指派相应级别的里程碑决策当局进行监管,如图8-1所示[ZL2001]。

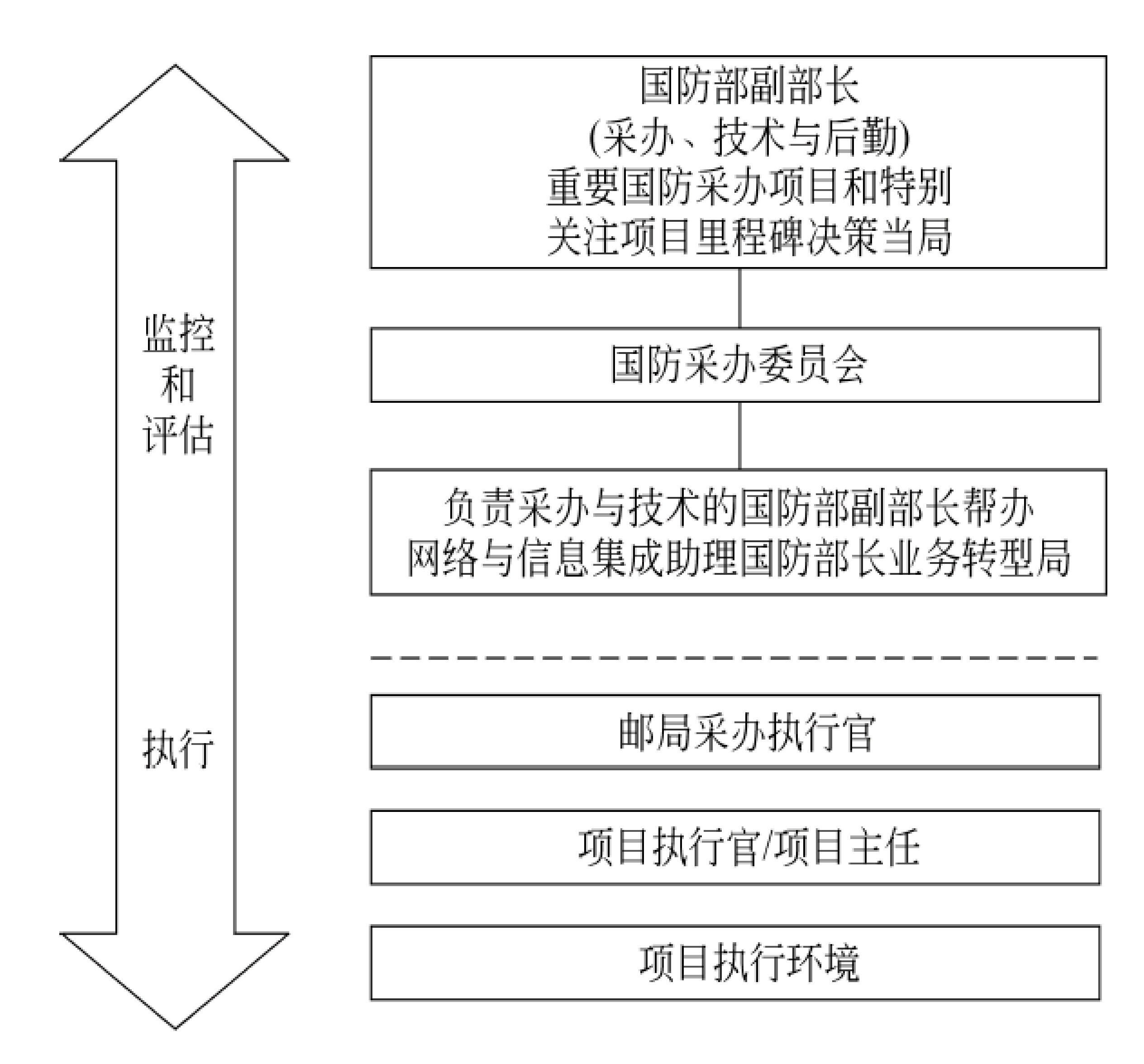


图8-1 不同类别的信息技术采办项目[ZL2010]

美国建立了以国防部为主,其他有关政府部门为辅的系统庞大的武器装备采办管理体系。国防部是集中统一管理部门,三军负责具体组织实施,三军均设有主管武器采办政策计划的主管部门和相应的采办实施部门。除了国防部,其他有关政府部门也参与武器装备采办和国防工业管理。其中,能源部是主管核武器工业的政府部门,负责管理核武器系统的研制生产,主管核武器项目的是负责国防计划的助理部长;国家航空航天局是美国民用航天业务的主管部门,并承担一部分军用航空航天计划,运输部是美国使用运输交通业务的主管部门,该部的“船舶管理署”负责船舶工业(包括舰船工业)的管理和协调[ZL2010]。

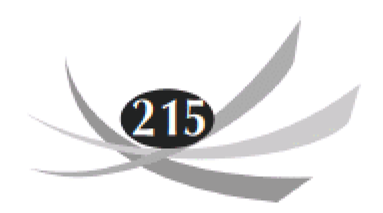
近年来美军服务采办费用持续上涨,其经费使用效益值得关注,因此,美军意识到需对采办服务进行严格的审查监督。国防服务采办属于政府行为,对采办项目的审查监督属于行政手段。法治国家中,在政府行为过程中使用行政手段必须要有明确的法规依据。近年来美国不断完善服务采办审查监督的法规体系,如表8-2所示。

表 8-2　相关法规[LW2011]

法规执行主体	法 规 名 称	在服务采办审查监督方面的规定
国家层次	《联邦采办条例》[FAR]	1. 政府有权限监督所有服务合同,拒绝不达标的服务 2. 制订质量保证监督计划及服务质量标准 3. 合同文本中包含质量标准
国防部层次	《2002 年国防授权法案》[NDAAF]	要求国防部建立服务采办的审批程序
	《联邦采办条例国防补充条例》[DFARS]	1. 配备技术代表,辅助合同官进行承包商选择和服务绩效监督 2. 对于金额超过简化项目标准的服务采办项目,合同文件中须包含《质量保证监督计划》计划中应明确绩效风险,说明在合同中增加哪些条款可以降低绩效未达标的风险
	负责采办、技术和后勤的国防部副部长政策备忘录《服务采办》(2002 年发布)[USD(AT&L)]	20 亿美元以上的服务采办项目由负责采办、技术和后勤的国防部副部长审批,其他项目由各军种审批,各军种要制定自己的审批程序
	《国防采办系统的运行》中的附件 9:《服务采办》(2008 年发布)[ODAS]	总结 2006 年服务采办政策基础并添加同行审查机制
	负责采办、技术和后勤的国防部副部长政策备忘录《服务采办的审查标准》(2009 年发布)[USD(AT&L)]	规定了合同签订前决策层审批和同行审查的标准,以及合同签订后同行审查的标准
军兵种层次	陆军 AR70-13 号规程《服务采办的管理与监督》 空军《采办与保障的全寿命周期管理》中第:4 章:服务采办海军指令中第 8 章:服务采办	指定军种内部的服务采办审批主体,明确各部门职责,介绍监督管理政策
	陆军《供应与服务合同的同行审查》 海军《同行审查计划》 空军《供应与服务合同的同行审查》	规定军种级别的服务采办同行审查政策

从法规文件体系来看,上述法规体系由条例、指令、规章以及政策备忘录等构成,较为完整,为后续法规的制定和细化提供了框架。从法规执行主体来看,国家、国防部、军兵种等各层次均能有法可依,有规可循。各机构内部依据法规指定审查监督主体,从而形成了服务采办监管的组织体系。从法规具体内容来看,法规体系起到了如下作用:首先是保证高层权力的介入,加强审查力度;其次是强调审查监督的独立性,保证实效;第三是确立了以合同官、合同官代表为主的监督责任体系,并将监督计划归入正式合同文件之列,使得审查监督制度化[LW2011]。

奥巴马政府上台以来,面对装备采办领域严重的"拖进度、降指标、涨费用"问题,不断



推进采办管理改革，要求军方加强对采办过程的审查监督力度，颁布了《武器系统采办改革法》，并酝酿对信息系统采办的管理体制与运行程序实施改革。针对装备采办中广泛存在的问题，奥巴马明确提出要对采办系统实施“强有力改革”，并积极推动相关的立法工作，美国国会两院进行了《2009 年武器系统采办改革法》（简称《改革法》）的立法，并于 5 月 22 日由奥巴马正式签署生效。《改革法》要求加大项目实施过程中的系统工程、技术管理与试验鉴定力度，重组系统工程和研制试验鉴定机构，进一步加强装备技术成熟度管理，降低装备项目技术风险。奥巴马政府强调“均衡务实”的国防政策，在 2010 年 2 月发布的《四年一度防务评审》报告中指出，在采办管理改革中注重协调多方关系，强调采办过程管控与快速高效的平衡，立足国内采办与加强国际合作的平衡，不断提升部队完成多样化任务的能力，持续推进采办管理制度的优化和完善[WL2010]。

8.4.2 美国国防部的 ICT 采办系统

国防采办的过程就是满足军工产品需求的过程，其实质上指的是满足国家安全需求的过程。美国是世界上的军事强国，在采办理论和政策上一直处于前沿。1971 年，美国国防部就发布了第一份关于采办的报告，时至今日，美国政府已经对这份报告做了 7 次重大的修改，从中足以体现出美国对历史经验的总结和对未来的规划[SHC2007]。

美国国防部共有三个分系统来组织国防 ICT 采办，这三个系统互相配合，来完成军工产品的 ICT 采办，它们分别是规划、计划预算与执行系统（Planning，Programming，Budgeting and Execution，PPBE），联合能力集成与开发系统（Joint Capabilities Integration and Development System，JCIDS）和采办运行系统（Defense Acquisition System，DAS）。

PPBE 系统是国防部战略规划，项目开发和资源分配的过程，其目的是为了更好地在美国国防部内部进行资源分配。事实上，有关规划、计划与预算的系统（PPBS）早在 20 世纪 60 年代就已经被用作军事领域。它把规划、计划和预算 3 个阶段的工作有机地结合起来，统筹的考虑军事战略、武装力量结构、武器装备和资源分配，从而能够科学合理地分配有限的资源。作为 PPBS 系统的衍生物，PPBE 系统保留了 PPBS 原有的特点，但将更多的重点放在国防部对国会批准预算（该预算由 PPBE 系统产生，并由总统签发）的执行上，更加重视评估对过去预算经费的收益情况，这样就弥补了 PPBS 系统不太重视经费的使用效益的缺陷。

PPBE 系统能更好地评估国防部批准的计划项目是否产生了预期效果，更好地实现了资源分配决策，从而实现 PPBE 系统的最终目的：在规定的财政预算限制范围内，为作战指挥官提供人员、装备、后勤保障的最佳配置。由此可见，美国国防部利用 PPBE 系统来实现资源的有效配置。计划、预算与执行审查阶段的并行大大缩短了工作周期，提高了采办效率[LL1999]。

JCIDS 是一种基于能力的分析系统，通过该系统对武器装备的发展需求进行分析，可以走出“先列装再系统集成”的误区，这就使武器装备具有从采办的最初就具有了联合能力，从而从装备建设的源头解决了不同军种，不同部门在武器装备上的重复采购、资源浪费，实现了系统互联、信息互通、功能互操作等方面的问题。这对于美军转型以满足未来

信息化战争非常重要[WE2007]。

联合能力集成与开发系统(JCIDS)的重要功能是在能力开发初期就进行了必要的功能分析。整个分析过程以国家防御政策和通用的联合作战框架为基础,通过分析现有联合部队作战行动、DOTMLPF(条令、机构、训练、装备、领导和培训、人员以及设施)和政策的能力与不足,确定联合作战能力现有或未来的差距,寻求能够解决这些差距的可能方案,同时还针对每一种可能的方案,粗略评估联合部队的成本和行动效果,为进一步分析提供基础[JCIDS]。

为此,JCIDS 的主要分为 4 个实施阶段:功能领域分析(FAA),功能需求分析(FNA),功能解决方案分析(FSA)和后期独立分析(PIA)[JCIDS]。

FAA 的目的是描述需要做什么。它将确定为实现某一目标所需要的作战任务、条件和标准。它以国家战略指导方针、联合未来概念集、统一指挥计划规定的任务、作战概念、联合任务、能力列表、敌方主要能力的预想范围及其他资源为输入,经过分析得到一个有优先级的涵盖所有功能领域的能力和任务列表。这些能力将构成综合体系结构的基础。

接下来进行的是 FNA,该过程通过比较需要做什么和现在有什么,描述了联合能力的差距和冗余在哪里。它利用 FAA 的输出作为基本输入,对已有的和正在设计中的作战系统所能发挥的联合能力进行评估,分析目前的能力与所需要的能力之间的差距和冗余,得到一个有优先级的能力差距列表。同时,作为定义能力需求的一部分,FNA 需要对整个范围的 DOTMLPF 和政策进行评估。

FSA 的输入是 FNA 确定能力差距列表,并为此输出可能的解决方案。

整个评估过程的最后一步是 PIA,它将对先前所做所有的分析进行检查,从而确保其完整全面性,并对推荐的各种方案进行评估以确认其是否具备弥合能力差距的可能性、可行性。对于装备方案,评估所得的结果将记录在 ICD(初始能力文件)中,供后续阶段进行再优化并开展相关研制工作使用;而对于非装备方案,评估所得的结果则将被记录在 DOTMLPF (非装备方案计划)改革建议中。

作为三个国防采办系统中的最后一个,DAS 是国防部获得武器和自动化信息系统的过程。这一过程提倡在坚持原则及解释责任的前提下,进行权力下放并简化采办流程,从而实现更具有灵活性和创新性的采办。DAS 分为系统采办前期、系统采办和系统维持等 3 项活动,如图 8-2 所示,设置了方案精选、技术开发、系统研制和验证、生产和部署以及使用与保障等5 个阶段,并分别在第二、第三和第四阶段前设 A、B、C 三个里程碑决策点[DoD 5000.1]。

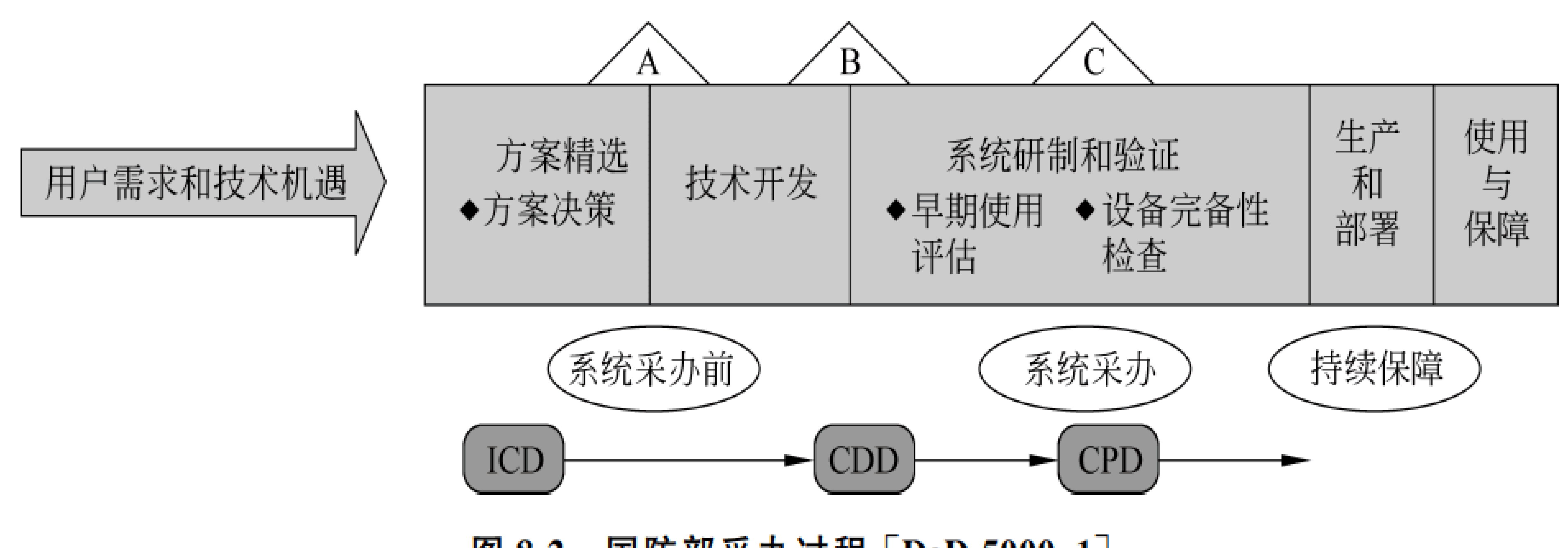


图 8-2 国防部采办过程[DoD 5000.1]



采办项目可从里程碑决策点 A、B 或 C 进入采办程序,可采用渐进式采办或一步到位采办。但在进入各阶段前,必须满足预定的“进入准则”[DoD 5000.1]。

在进行方案精选之前,首先要做的是方案决策。方案决策根据 JCIDS 系统提供的初始能力文件(ICD)所反映出的武器装备需求,对多种可能方案进行全面的分析、遴选。而对于方案的遴选,是通过国防科学与技术(S&T)计划实现的[DoD 5000.1]。

当项目进入到“方案精选”阶段时,工作便会转交到国防部领导层由其组织进行论证、精选“备选方案分析”计划,评估各方案的技术成熟度、技术风险和必要的技术成熟性演示验证要求等因素,选出最佳方案。在 ICD 和备选方案分析计划的指导下,通过对采用渐进还是一步到位采办方式的选择,拟定科技发展战略,到达里程碑 A。里程碑决策点 A 的任务就是控制项目进入技术开发阶段,如果里程碑决策者批准方案及科技发展战略,该项目将进入技术开发阶段。

降低技术风险是技术开发阶段的重点,它应保证系统在五年内能够适应整个采办体系不断变化,从而相应的做出生产改进,详细的规划成为成功的关键。当技术开发阶段得出最终的能力开发文件,就到达了控制开始新的采办计划,进入系统开发与演示验证阶段的里程碑 B。通常,将方案精选阶段和技术开发阶段统称为系统采办前期。

里程碑 B 的决策者批准能力开发文件后,采办过程进入系统研制和验证阶段。这个阶段,将对系统进行早期使用评估,将经验证的各个分系统整合到完整的系统中,从而降低集成风险,同时进行技术审查,验证是否满足武器装备建设需求,是否具有实用性,互操作性,集成性。并以此为基础准备初始低速生产提案,到达里程碑 C。

在里程碑 C,里程碑决策者批准提案后,采办活动进入生产和部署阶段。首先将低速生产具有代表性的产品,并进行初始作战实验与评估和实弹试验与评价,并将报告提交国会,建立初始生产基础。国会批准之后,系统将进入全速生产阶段。在全速生产的过程中,仍将根据不断变化外的实际情况调节生产系统部署,同时要监督系统性能,纠正缺陷弥补不足以改善系统性能和保障,并适当地进行后续试验与评估。如果评估符合标准,则应对系统过去的表现再次进行评估。最终应建立稳定高效的生产和支援基地,实现初始作战能力,确保装备系统能够为作战人员持续提供所需能力[DoD 5000.1]。

在使用与保障阶段,应制定包含保持所部署武器系统待命状态和作战能力所需的一切因素的维持计划。实施后续作战试验与鉴定计划,以评定所部署系统的作战效能、生存能力、适应性和互用性,并发现存在的缺陷,及时对硬件和软件的进行改造和升级,维持部署系统的作战能力。

武器系统的使用期结束时,需向国防部再利用与市场营销办公室提供解除军事化的处置要求以及足够的资料,在不违反安全、保密和环境法规的情况下,对武器系统做最后的处置工作。同时,在采办程序 A,B,C 三个里程碑所产生的评审结果,都应及时反馈到“方案改进”阶段,以促使方案不断修正、达到完美。国防采办程序以加强方案论证为重点,以提高采办效率为核心,对于确定系统全寿命期采办管理最佳方案、使采办工作不走或少走弯路具有重要意义[SHC2007]。

这三个系统在美国武器装备的采办过程中相互支持、相互作用、相互制约。事实上,这个过程是非常复杂的,如果对每一个系统的运行模式以及各种管理机构之间的制约关系没有深入广泛的了解,就不可能对美国国防采办系统有一个清晰的认识[DAG]。

8.4.3 美国国防部ICT采办存在的问题

1. 组织机构间职责划分不合理

目前,国防部内信息技术的采办权力主要集中在3个部门:采办、技术与后勤副国防部长,网络与信息集成助理国防部长(兼国防部首席信息官),以及业务转型局。这种权力划分会造成以下这些问题:首先由于网络与信息集成助理国防部长的工作自主性很强,拥有直接向国防部长报告工作的权利,因此虽然名义上采办、技术与后勤副国防部长是信息技术采办的最高决策者,网络与信息集成助理国防部长在该副国防部长的授权下开展工作,但是由于这种职责划分的不合理,采办、技术与后勤副国防部长对信息技术采办的统管力度往往不足。其次由于各部门往往下设其他部门,使得部门之间产生管理混乱、权责不清、协调难度大、管理效率低等问题,与信息技术的快速发展不相适应。最后管理上的条块分割使信息技术专家分散于国防部各个部门,彼此间的沟通协调存在很大障碍,管理力量和专家资源分散,难以形成整体优势[ZL2010]。

2. 现有采办程序不适合

快速变化的信息技术任务要求几个月甚至几周时间就能完成军事能力部署。而美军在当前采办程序下进行的信息技术采办项目,几乎99%的项目周期都要超过1年。这说明当前的采办程序已经严重不适应快速发展的信息技术和不断变化的能力需求。造成这种情况主要是因为传统的采办模型已经不适应信息技术项目。美军当前的信息技术采办沿用硬件系统的采办程序,该程序将系统采办的生命周期划分为需求开发、方案分析、技术开发、工程与制造开发、生产部署和使用保障等几个阶段,规定了它们的先后次序与进入标准。采办活动严格按照线性方式进行,当项目经相关部门审核,确认完成了本阶段任务并且满足下一阶段的进入标准后才可向前推进,否则返回修改。这种模型的线性过程太理想化,不适合现代的软件开发模式。首先,项目各个阶段的划分完全固定,项目单线进行,效率不高。其次,项目早期的错误要等到后期的测试阶段才能发现,而用户也只有等到整个过程的末期才能见到开发成果,不利于在开发过程中对项目满足需求的情况进行监督,这往往造成项目风险偏大和成果不能满足用户需求等问题[ZL2010]。

3. 采办人员经验不足

一份对重要信息技术采办项目的调查显示,造成费用、进度、质量和性能方面问题的最主要原因是高级别领导者缺乏成功的信息技术采办经验。当前信息技术项目的领导者很多都是工程技术方面的专家,缺乏大规模的、信息技术方面的商业采办经验。项目过程中的决策行为主要是管理者基于过去经验的判断,所以拥有丰富经验的管理人才可以为项目成功提供良好的保证。当前,国防部各部局和军兵种内很多经验丰富的老专家即将退休,而新进入的专业人员不断减少,这将造成采办队伍中的管理经验严重流失。美军试图通过加强对在职人员的培训来解决这一矛盾,但目前收效甚微[ZL2010]。

针对美军采办的突出问题,可通过一些措施对ICT的采办进程进行优化。首先要清晰分配采办职权,清晰的职责和权利分配是实现信息技术采办高效快捷,确保采办项目能够更及时地反映需要的前提,因此通过合理的划分,进一步明确信息技术采办过程中的职责和权利分配,将会是ICT采办的主要工作。其次采取更适合ICT特点的采办程序。鉴于现有采办程序难以适应信息技术快速发展的现状,开发一套适用于信息技术项目的

专用程序对ICT采办发展来讲显得尤为必要。最后,也是十分关键的一步,是要完善采办人员选拔培养工作。具备丰富项目管理经验的领导者是正确进行项目决策、促进信息技术采办项目顺利执行的核心要素。因此不仅要提高项目领导者的信息技术水平,还要提高对领导者过去管理经验的要求,把这二者作为人员选拔、遴选的重要因素。信息技术在商业领域的发展速度较快,成功的商业模型对改进军队信息技术采办有很强的借鉴意义,所以要大力提倡结合成功的商业模型对采办人员进行培训[DSB2009]。

参 考 文 献

[DSB2009] William Schneider, Jr. Department of Defense Policies and Procedures for the Acquisition of Information Technology. Report of the Defense Science Board Task Force on. March 2009.

[LW2011] 李维.美国国防服务采办审查与监督策略研究.装备指挥技术学院学报,2011.

[ZL2010] 周磊.美军信息技术采办管理现状、问题及改革趋势.装备指挥技术学院学报,2010.

[ISO/IEC17799] Val Thiagarajan B. E. Information technology-Code of practice for information security management. SANS Institute, August 2010.

[NIST SP 800-59 2003] William C. Barker. Guideline for Identifying an Information System as a National Security System. National Institute of Standards and Technology, August 2003.

[NIST SP 800-53 2009] Recommended Security Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology, August 2009.

[L2001] 总装备部情报研究所.美、英、法、德、日国防采办系统比较.中国国防科技信息中心研究报告,2001年.

[XY2009] 游客.IT采购有三大忌讳.NETWORK&INFORMATION,2009: 23(9).

[YK2009] 夕阳.IT采购三大新趋势.NETWORK&INFORMATION,2009: 3(9).

[YXG2008] 俞晓国.供应链管理下建筑业采购模型构建与比较.哈尔滨工业大学学报,2008.

[SHC2007] Stephen Howard Chadwick. Defense Acquisition: Overview, Issues, and Options for Congress, CRS Report For Congress, June, 4, 2007. http://www.fas.org/sgp/crs/natsec/RL34026.pdf.

[LL1999] Leslie Lewis. Planning, Programming, Budgeting and Execution System (PPBES). Rand, 1999. http://www.dtic.mil/whs/directives/corres/html/704514.htm.

[WE2007] Willian E. Gortney. Chairman of the Joint Chiefs of Staff Instruction 3170. 01F, May 2007. http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf.

[ODAS] Operation of the Defense Acquisition System. 2008.

[JCIDS] JCIDS overview. 18 Oct, 2004. http://www.mors.org/meetings/cbp/read/3170%20Brief%20to%20MORS%2018%20Oct%20041.pdf.

[NDAAF] National Defense Authorization Act for Fiscal Year 2002. 2002.

[USD(AT&L)] Under Secretary of Defense(acquisition, technology and logistics, USD(AT&L)). 2002.

[DoD 5000.1] DoD Directive 5000.1. The Defense Acquisition System. May 12, 2003. https://akss.dau.mil/dag/welcome.asp.

[DAG] Defense Acquisition Guidebook.

[FAR] Federal Acquisition Regulation. FAR, 2010.

[WL2010] 王磊. 奥巴马政府上台后美军装备采办管理与改革. 国际航空,2010.

第9章 ICT外包安全

9.1 概　　述

1989年,全球知名的影像处理公司 Eastman Kodak 公司将其整个的数据中心、网络以及微机操作业务分别外包给 IBM、Digital Equipment 和 DEC 等公司,这项为期10年、总值2.5亿美元的外包合约成为企业 IT 外包发展的里程碑。自此以后,越来越多的组织认识到利用信息技术获得战略优势在于如何应用信息技术,而不在于是否拥有信息技术,信息技术外包得到了蓬勃的发展。ICT 外包战略确实给一些企业带来了很大的经济利益,但是也有一些企业因为 IT 外包而给企业带来了巨大的损失,在外包过程中,很多外包企业和他们的伙伴对合约原始条款进行了再谈判,其中相当一部分的谈判以失败告终,之所以如此,一方面是由于 ICT 外包合约的复杂性,这种复杂性来自于与外部供应商建立的长期关系以及企业资产被置于外部行为人的控制之中。另一方面也是由于 ICT 外包中存在的信息不对称以及道德风险。因此,研究 ICT 外包中的风险及其特征对于提高 ICT 外包成功率及加强对 IT 外包的管理具有重大的理论和实践意义。

随着企业信息化的深入发展,ICT 部门已经成长为企业的一个重要部门,ICT 的作用逐渐从“提高效率”的目的,即为企业提供支持性服务转变为“提升效果”的目的,从而使得 ICT 具备战略性价值。传统上,企业获取 ICT 能力采用完全内制的方式,这种内制的方式由于在 ICT 需求和 ICT 供给两个方面均缺乏有效约束,容易使 ICT 部门成为企业的“投资黑洞”。数十年来,随着全球企业信息化的持续投入,ICT 支出已经成为企业的第三大费用支出。90年代以来,在企业资源观的理念和归核化思潮的带动下,业务外包模式开始在世界范围内兴起,ICT 外包作为业务外包的一种在这种背景下应运而生。外包是分工整合模式下组织企业资源的有效方式,美国著名管理学者杜鲁克曾预言:“在10年至15年之内,任何企业中,仅做后台支持而不创造营业额的工作都应该外包出去,任何不提供向高级发展的机会的活动、业务也应该采用外包形式”。

供应链外包战略的理念是:如果企业制造链上的某环节不是世界上最好的,如果这又不能为我们带来竞争优势,那么就将其外包给该行业最好的专业公司来做,从而为自己集中于本公司核心业务释放了资源、分散了风险,同时也提供了供应链的市场共赢。因此,供应链外包战略的选择首先必须确定本公司的核心竞争力。核心竞争力就是既能给组织带来明显的竞争优势,又能全面反映组织的技术和文化的一些基本特征。核心竞争力一般具备如下三个特征。

(1) 高独特性:促成企业竞争力的资源能够被企业组织单独拥有,企业能够从中获

得长期的租金,这些资源可以是设备、技术、专利或技能的集合;

(2) 低取代性:促成竞争力的资源很难被相关的技术、专利或方法所模仿或取代;

(3) 高收益性:由核心竞争力所带来的收益是巨大的,为公司在某一领域保持较高的收益。供应链的决策要与企业核心竞争力的确定紧密结合,突出核心竞争力的产品部件必须保留在企业之内生产制造。当进行外包决策时,如果企业注重核心竞争力,那就不仅仅意味着外包制造,而且也意味着外包设计。这样,在新产品设计开始时就制定这些决策显得至关重要,供应商也由此从一开始就可以参与进来。

对于一个希望从供应链外包战略中获取最大经济效益的企业来说,根据企业的发展要求和产品特点进行正确的外包决策之外,还必须兼顾实施过程中的不同外包决策的组合,才能够获得最优效果。此外还必须和供应商合作战略有机的结合,加强激励,建立和优化信息沟通渠道,保证供应链整体决策优化等,才有可能保持企业在供应链中的整体竞争力。

9.2 ICT外包基础

ICT外包是指组织为了实现自己的目标,通过合同或协议的方式将部分或全部的信息技术职能交由外部的服务提供商提供的一种管理模式。ICT外包一般还伴随着企业的ICT资产、人员、租赁资产交由ICT服务商管理。常见的ICT外包包括ICT应用开发和维护、通信网络管理、信息系统运作和管理、ICT设备维护、备份和灾难恢复以及ICT培训等[K2010]。

国内外学术界,特别是国外如美国、西欧等在ICT外包领域的研究已经取得一定的成果,我国作为一个高速发展中的经济体,是潜在的ICT外包大市场,迫切需要ICT外包理论的指导。因此,在吸收、消化国外学者研究成果的基础上,结合中国ICT外包的具体实际,从理论的高度系统化地研究ICT外包问题,进而指导我国企业ICT外包实践,是增强我国企业竞争力的重要方法。

9.2.1 ICT外包简介

在ICT外包成为一种重要的商业现象的同时,学术界也有越来越多的人将目光放在这上面,在较短的时间内,就出现了大量的研究文献,研究的话题,也非常广泛涉及到了外包的理论基础、外包的收益、风险、外包决策、外包过程管理等诸多方面,甚至有学者从政治的角度研究外包对国家安全的威胁。总体来看,业界通常将外包大致分为三种类型:(1)同时从客户和服务商的角度研究完整的ICT外包活动;(2)从服务商的角度研究应用服务提供(Application Service Providor,ASP)这样一种特定的ICT外包服务形态;(3)研究离岸外包(Offshore Outsourcing)这样一种特定的ICT外包服务形态[K2009]。

从逻辑上看,ICT外包服务就是满足客户ICT外包的需求,其定义应与ICT外包相对应,目前理论界从客户的视角对ICT外包有两类不同的定义。

Lacity和Hirschheim于1993年在Sloan Management Review上将ICT外包描述为从外部采购原来由企业内部提供的产品和服务。其后许多文献都沿用了这一定义。如

果按照此类定义，外包与企业原本的业务是相关的，它是对企业业务的一种转移。简单地说，如果有些业务原来是由企业内部完成，现在改为企业外部完成，这种转移过程称为外包，如图 9-1 所示。打个比方，如果某企业需要使用信息管理软件，而它又不打算自行开发，现在该企业将信息系统的开发委托给软件开发商。那么从上述定义的角度上来说，由于采购的并不是原来企业内部提供的服务(企业内部原来没有此项业务)，因此，将信息管理软件委托给软件开发商进行开发并不能认为是软件开发外包。另一方面，假定某企业过去已将部分 ICT 业务委托给了外部服务商，经过相当长的时间后，使用外部资源已成为常态，此时使用外部资源也不能称为外包[LH1993]。

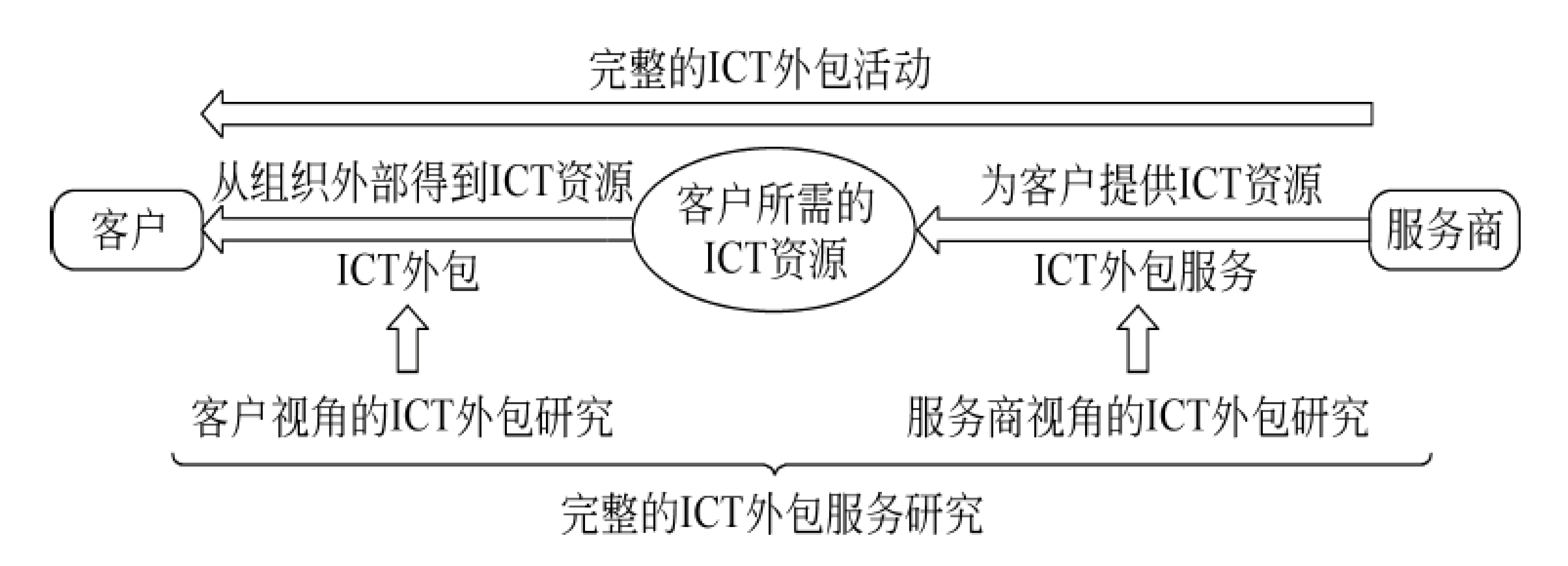


图 9-1　外包与 ICT 外包服务的区别和联系[LH1993]

Loh 和 Venkatraman 将 ICT 外包定义为“外部服务商提供实物和人力资源承担用户组织的部分或全部信息技术基础设施的服务方式”。这个定义更好地体现了 Outsourcing 一词的本来含义。Outsourcing 与 Insourcing 对应，它的原意是从外部取得所需的资源，这种对外包的定义，强调的是企业为获取所需资源采取的一种战略安排，它并不关注资源的获取过程。只要企业从外部得到所需的服务，不论这些服务原来是否由企业自己提供，都是外包服务[LV1992]。

9.2.2　ICT 外包类型

ICT 外包服务已经是一种比较普遍的商业服务，对它进行分类即有助于根据各种外包服务的具体情况进行讨论，又有助于认识它们共有的本质特征，对研究对象进行分类也是最基本的研究方法之一。从分类方式上看，采用多个指标，从不同的视角来分类更有利于讨论具体业务中的特定问题，对理论研究和服务商的市场区隔实践都有指导意义。

(1) 根据客户与外包商建立的外包关系可以将 ICT 外包划分为：市场关系型外包、中间关系型外包和伙伴关系型外包。

罗伯特·克莱珀和温德尔·O·琼斯在其《信息系统、技术和服务的外包》一书中将外包合同关系视为一个连续的光谱。其中一端是市场型关系，在这种情况下，你的组织可以在众多有能力完成任务的外包商中自由选择，合同期相对较短，而且合同期满后，能够在成本很低或不用成本、很少不便或没有不便的情况下，换用另一个外包商完成今后的同类任务。另一端是长期的伙伴关系协议，在这种关系下，你的组织与同一个外包商反复订立合同，并且建立了长期的互利关系。而占据连续光谱中间范围的关系必须保持或维持合理的协作性，直至主要任务的完成，罗伯特·克莱珀和温德尔·O. 琼斯将这些关系称为“中间”关系。由于这是一个连续光谱，有些关系靠近市场关系，有些关系则靠近伙伴关

系，而在两端之间就是中间关系。

这两位学者对以上各种关系的适用性作了分析，他们认为：与外包商建立的关系类型取决于资产专属性、不确定性和续签合同的问题。资产专属性是指构成外包交易一部分的资产，这些资产是与特定外包商的外包协议所特有的，如果交易破裂，资产的生产能力就会削弱。

如果任务可以在相当短的时间内完成，环境变化搅乱需求的几率很小，而且没有什么真正的资产专属性，这样就可以订立一份规定了所有偶发事件的合同，此时，市场关系是适当的。

如果外包任务需要花费一些时间来完成，环境的变化可能改变需求，以及存在某些资产专属性，但是任务完成后，维持与外包商的关系没有任何特殊优势，中间关系型外包就是适当的选择。

如果完成任务持续的时间较长，相关需求会随着不可预见的环境变化而变化；资产专属性很高，以及与外包商续签合同能够最好地满足需要，这时就应当考虑伙伴关系型外包。在伙伴关系中，赢得另一方回报的信任和互利行为可以获得延续。管理成本和风险很高，因而伙伴关系带来的收益必须足以抵消这些成本和风险。例如，用户和外包商共同投资成立公司而建立的长期关系等[ML2009]。

(2) 按照 ICT 外包的程度可以将外包划分为整体外包和选择性外包。

整体外包系指将项目的 80%或更多外包给外包商，选择性外包是指几个有选择的职能的外包，外包数量少于整体的 80%。整体外包因为牵涉的范围很广，风险是很高的，由于整体性外包合同往往要持续很长的时间（通常超过 5 年），而且整体性外包的用户必须花费大量的时间、精力和资金来分析外包交易并与外包商洽谈合同，另外整体性外包可能会导致信息技术灵活性的大幅度削弱，所以任何组织选择整体性外包时都必须三思而行。

(3) 按照价值中心的方法可以将 ICT 外包划分为成本中心型、服务中心型、投资中心型和利润中心型外包。

成本中心型外包是指通过 ICT 外包在强调运行的效率的同时使风险最小化。服务中心型外包是指通过外包在使风险最小化的同时建立基于 ICT 的业务能力以支持组织的现行战略。投资中心型外包是指通过 ICT 外包使组织对创建新的基于 ICT 的业务能力建立长期的目标并给予长期的关注。利润中心型外包是指通过 ICT 外包向外部市场提供 ICT 服务并获得不断增长的收入并为成为世界级的 ICT 组织获得宝贵的经验。

(4) ICT 服务的提供者有硬件厂商、软件企业、专业的 ICT 服务提供商和电信服务提供商。将 ICT 外包服务的业务类型分为以下 9 大类。

- 运行维护：它的服务对象从单台设备、软件到整个复杂的信息系统；运行维护工作包括排除设备硬件故障、软件安装、系统日常维护，系统优化等多种级别。不过，产品保修期内或新建系统维护期内由厂商提供的服务不是外包服务。
- 软件定制开发：包括产品开发、产品支持、软件升级和优化、软件本地化、软件测试、网页制作等许多子类型。与硬件产品的维修相似，由开发者或销售者提供的例行性的产品升级服务不是独立存在的外包服务。
- 系统集成：这是中国 ICT 企业很关注的一类服务，目前国内研究主要沿用 IBM

公司对系统集成的定义,讨论如何将一个企业内的计算机、网络设备和软件等要素组合成一个有机的信息系统。国外早期的文献对企业内部信息系统的集成问题比较关注,但近来的文献主要集中在探讨企业合并、供应链管理等背景下的信息系统的整合等问题。

- ICT 咨询:既有偏向于技术方面的为客户提供 ICT 架构的咨询和应用系统的咨询,也有偏向于管理的 ICT 与业务部门沟通的咨询,当然也有两者兼顾的 ERP 实施的咨询等服务。
- 安全服务:包括系统认证、渗透测试、风险评估、应急响应、安全响应、安全加固、信息安全监控中心(Security Operation Center, SOC)、顾问咨询等子类型。
- 派遣服务:服务商向客户派遣工作人员,这些人员的工作是在客户指定的地点完成客户分配的任务。派遣人员的身份是服务商的员工,对他们的培训、福利和其他烦琐的人力资源管理由服务商完成。
- 专业培训:在客户企业的 ICT 设施没有完全外包给服务商的时候,客户企业需要由掌握了专业知识的人来规划、建设或维护这些设施;即使客户实施了全面的 ICT 外包战略,也需要专业人员来监控系统的正常运行并作为企业的代表与服务商沟通。信息技术的发展速度非常迅速,ICT 人员的知识更新周期缩短,专业培训服务也就应运而生了。专业培训服务又可分为两类,一类是通用的信息技术培训,如计算机操作、程序设计、项目管理等等,另一类则与特定的软、硬件有直接的联系。
- 电信服务:包括互联网接入服务,网络连接服务(如为银行营业点与总部的通信提供租用线路),在传统电话网的基础上开通的电话虚拟专网服务,即时消息通信服务,集团短信服务等多种类型。提供电信服务的服务商不但有传统意义上的基础电信运营商(如中国电信、中国移动等公司),还包括腾讯、微软(其 MSN 业务)等新兴的增值电信运营商。
- 托管服务:上述外包服务的共同特征是 ICT 设施的所有权属于客户,服务商到客户指定的地点提供服务。如果 ICT 设施的所有权和维护责任都交给了服务商,或者将 ICT 设施转移到了服务商指定的地理位置,服务商提供的就是托管服务。在此定义下,应用服务提供(ASP)、主机托管、主机租用、信息系统租用等服务都属于托管服务。

服务方式的差异是指不同服务商提供相同服务时采用的技术及管理模式是否相似,服务成果的不确定性是指同一服务商用相同方式为不同客户提供服务时服务成果是否相似,它与客户的配合情况有关,也与服务成果的度量方式有关。电信服务的差异程度最低,对客户配合的要求比较确定,服务质量较易用一些公认的指标来表征,结果的不确定性最小;ICT 咨询服务则处于另一个极端。软件定制开发是一个独特的领域,其中有些服务(如编程服务 Coding Service)的服务方式差异较小(标准化程度较高),另一些服务(如系统开发)的标准化程度较低;它的服务质量不易评价,服务成果与客户有很大的关系,不确定性较大[RW1998]。

9.2.3 ICT外包理论

在国内外学者对ICT外包的研究中,无论是对ICT外包的目标、对象,还是对ICT外包的合作伙伴、ICT外包的管理方面的研究,均从一种或者多种理论视角出发对ICT外包的各个方面进行解释。这些支持性理论主要包括资源基础理论、核心能力理论、资源依赖理论、委托—代理论和交易成本理论,每一种支持性理论均从自身的理论视角出发对ICT外包的某个或多个方面进行解释和论证。以下从ICT外包主要支持性理论的研究视角进行简单的综述。

1. 核心竞争力理论

在现有的研究文献中常使用核心竞争力理论来解释客户寻求ICT外包的动因:企业在决定是否外包ICT业务时主要考虑到通过外包能在硬件、软件和人力资源上节省开支,更快地升级或部署新的应用,或者让应用更具可伸缩性;将战略集中于核心能力更是企业考虑将部分或全部ICT业务外包的重要理由,如果无法在企业内部满足对ICT的需求或不将其作为核心能力时,企业就可能寻求外包的解决方案。

1990年,提出了核心竞争力(Theory of Core Competencies)的概念——"核心竞争力"按照Prahalad和Hamel的定义,企业的核心能力有三个基本特征:核心能力提供了进入多样化市场的潜能;核心能力应当对最终产品中顾客重视的价值做出关键贡献;核心能力应当是竞争对手难以模仿的能力。

1957年美国学者Philip Selznick首次用"独特竞争力"来描述企业在执行既定战略时的某种技能,他把这种独特竞争力定义为组织在其发展过程中形成的特殊能力。Prahalad和Hamel发表了《企业的核心竞争力》一文,全面阐述了核心能力的思想,标志着核心能力理论的正式提出。他们认为核心能力是有利于企业发展的各种技术、技能的总和,是一种稀缺的、独特的、有延展性的能力,是企业竞争优势的源泉。是"在组织内部经过整合了的知识和技能,尤其是关于怎样协调多种生产技能和整合不同技术的知识和技能"。核心能力理论主要观点如下:第一,在本质上企业是一个能力集合体。企业的能力是企业长期积累和学习的结果,而企业的核心能力是企业拥有的最主要的资源或资产,它的储备状况决定着企业的经营范围,它的差异决定着企业效率的差异,从而最终决定企业的收益差别。第二,企业拥有的核心能力是企业长期竞争优势的源泉。企业的长期竞争优势其实是单个企业拥有比竞争对手能够更高效地从事生产经营活动和解决各种难题的能力,现实的经营战略、组织结构、技术水平等优势只不过是企业发挥智力资本潜能的产物。第三,积极培育和运用核心能力是企业的长期根本性战略。在信息经济时代,任何企业单是依靠某一项或某几项职能战略(如企业的市场战略、产品战略、技术战略等),最多只能获得一时的优势,唯有追求核心能力才是企业永久立于不败之地的根本性战略。按照Prahalad和Hamel的定义,企业的核心能力有三个基本特征:核心能力提供了进入多样化市场的潜能;核心能力应当对最终产品中顾客重视的价值做出关键贡献;核心能力应当是竞争对手难以模仿的能力。

Sony公司在微小型化方面的核心能力是一个著名的范例——具有将无线设备做到芯片上的理论知识并不能保证公司生产出名片大小的收音机。为了制成产品,公司必须

整合包括微小型化、微处理器设计、材料学和精密封装等各方面的知识与经验。在这方面的能力又可以应用到微型计算器、袖珍电视和数字手表等多个方面。与企业内的实物资产不同,不会由于将核心能力用到多个方面而使其有所损耗,相反还会进一步增强这种能力。Strickland 和 Thompson (2001)发现核心能力不会自然而然地出现,它必需被有目的地创建和培植。Saunders 等认为要整合学习以及信息共享并经过很长时间才能逐渐建立起核心业务或核心竞争力,追加大笔投资也不易使其迅速增强,也不容易转移给他人或被模仿。通常认为组织决不应将核心业务或核心能力外包出去[PH1990]。

核心竞争力理论为 ICT 外包提供了基础和目标。Quinn 和 Hilmer 指出,企业应将不具备核心能力的业务外包给其他企业完成,而把投资、发展的重点持续放在具有核心能力的业务上。只有真正具有战略重要性的产品或者服务应当留在企业内部完成,而其他的业务则应该外包,交给针对这些业务的一些专业组织来处理。核心竞争力战略的基本思路就是把企业的业务归拢到最具竞争优势的行业、把经营重点放在自己优势最大的价值链环节上,以实现利润的最大化。核心竞争力战略并不意味着产品品种的简单减少,它主要是开发、培育和利用企业的特有资源和能力。企业的特有能力体现在不同侧面,例如产品、技术开发、营销体系、管理水平和企业文化等。目前,核心竞争力理论已经成为各企业实施外包的主要动力和首要考虑因素[MAH2011]。

2. 竞争战略四因素理论

在 1980 年出版的《竞争战略》一书中,Michael Porter 指出制定竞争战略意味着要考虑四种关键因素,整体性、长期性、基本性,计谋性。竞争战略就是对竞争中整体性、长期性、基本性问题的计谋,发展战略就是对发展中整体性、长期性、基本性问题的计谋。这四种关键因素决定了一个公司可以取得成功的限度。

公司的强项与弱项是其资产与技能相对竞争对手而言的综合表现,包括财力资源、技术状况、商标知名度等等。一个组织的个人价值是主要的执行经理以及其他执行既定战略所涉及的人员的动机和需求体现。公司的强项与弱项与价值标准相结合决定了一个公司能成功地实施竞争战略的内部(指公司内的)极限。

外部极限是由产业及更大范围的环境决定的。产业机会与威胁决定了竞争环境。这种环境既伴随着风险,又蕴含着回报。社会期望是对公司产生作用的如下因素的反映:政府政策、社会关注、演变着的风俗以及其他一些社会因素。

Porter 将企业间关系作为竞争关系的假定受到学者的批评(他后来的著作对此进行了修正),企业也并不总是按照他的理论来决策。但是企业决策时都会自觉不自觉地考虑这四方面的因素,研究者用这一理论解释了许多企业的战略决策问题。笔者认为,企业之所以提供 ICT 外包服务,就是因为考虑到了四因素中的一个或多个因素,从总体上看,竞争战略四因素就是提供 ICT 外包服务的动因。

如果具体到某一个或某一类企业,由于它们所面对的公司内、外部情况有很大的差异,每种因素对决策的影响作用是不一样的,所以还是有必要针对具体情况进行分析。

3. 资源基础理论

资源基础理论(Resource-Based Theory)是从资源、能力、竞争优势和持续竞争优势之间关系出发考察企业战略。就外包而言,战略与能力之间的差距就是外包存在的可能

性空间。Barney 根据资源异质性和不可移动性假设提出资源基础理论模型，从企业内部资源的角度说明持续竞争优势的来源。在此模型中，Barney 提出四个资源分析标准：价值性、稀缺性、不可模仿性和不可替代性。Barney 的观点有助于企业的外包战略分析。从资源基础论的观点来看，ICT 外包作为一种战略决策有助于填补 ICT 战略与 ICT 资源之间的差距。战略与能力之间的匹配是一个动态的过程，因而 ICT 外包的这种填补过程也是一个动态的过程。基于这种认识，学者们试图利用资源基础观理论来解释 ICT 外包的战略价值、ICT 外包对象的选择等等问题。如 Vital Roy 从资源基础论的角度出发对 ICT 外包进行了分析，认为 ICT 被视为企业的一种资源，ICT 资源的战略价值只能通过它所支持或者实现的活动来表现[B1991]。

4. 资源依赖理论

与资源基础理论不同，资源依赖理论从组织与环境的关系角度说明企业之间的依存关系。资源基础论假设没有组织是完全自给的，所有组织都在与环境进行交换并由此获得生存，因此对资源的需求构成了组织对外部的依赖，而资源的稀缺性和重要性决定了组织对环境的依赖程度。组织依赖理论为分析业务外包（包括 ICT 外包）与组织效果之间的关系以及组织与外包商的关系提供一个视角。在激烈的市场竞争下，由于对外部环境的依赖，组织间需要建立一种稳定的相互依存的关系，从而在一定程度上弥补企业自身资源的不足。对外部资源的依赖也是外包产生的动因之一。对于 ICT 外包来说，单靠企业自身拥有的资源无法建立起有效的信息系统，必须与外部服务商建立起稳定的伙伴关系才能更有效地利用外部的专业化资源。

Cheon、Grover 和 Teng 对资源基础理论和资源依赖理论进行了检验，并为外包找到了依据。他们认为，外包至少在某种程度上依赖于企业所需的资源及它获取这些资源的战略[CGJ1995]。

5. 交易成本理论

科斯（Ronald Coase）在其 1937 年的著作《企业的性质》中首次提出交易成本概念。他指出，由于交易活动的稀缺性，作为一种制度安排的市场运行是有成本的，即市场交易成本。由于管理活动的稀缺性，企业运行也要有一定的管理成本，称为企业内部交易成本。市场交易成本的内容主要包括：(1)记载交易中发现相对价格的成本，如获取和处理市场信息的费用，这是在交易准备阶段产生的费用；(2)为完成市场交易而进行的谈判和监督履约的费用，其中包括讨价还价、订立合约、执行合约并付诸法律规范而必须支付的有关费用；(3)未来的不确定性引致的费用，以及度量、界定和保护产权的费用。企业边界最合理状态就是市场的边际交易费用等于企业内部的边际交易费用，内部、市场交易费用的大小成为了决定企业边界的两个重要因素。

威廉姆森（Oliver Williamson）在其 1971、1973、1979、1981 和 1988 年发表的一系列论文中对交易成本的决定因素进行了分析、论证和总结，最终形成交易成本理论（Transaction Cost Economics）。他进一步地对交易成本的决定因素进行分析，在提出有限理性和机会主义的人性假设之下，他认为交易成本的决定因素包括资产专用性、交易的不确定性和交易频率，其模型为交易成本的定量研究提供了很好的基础。不少学者将交易成本理论应用于外包理论的研究，ICT 外包与否被视为一种基于交易成本的选择，如



Wang,Eric T.G.以交易成本为理论视角,通过实证的方式对ICT外包成功的关键相关因素进行分析;类似的还有Soon Ang和Beath的研究。

企业组织存在的根源是企业内部化行为与外部交易行为之间的绩效比较。进入网络经济时代之后,网络通信、标准化、电子商务、系统集成、敏捷制造等使经济运行方式发生了重大变革。信息技术的发展使得企业的信息搜寻、获取以及发布的成本大为降低,即加速了市场交易费用的下降,当边际交易费用=边际组织费用,企业通过"内部化"节约的交易费用正好为管理费用的增加所抵消时,企业就会停止扩大其边界,而通过市场寻求获取资源,外包也就应运而生。

6. 代理理论

委托代理理论于20世纪60年代末70年代初由Ross、Mitnick、Jensen和Meckling创立和发展。在传统的阿罗-德布鲁体系中,企业被视为一个"黑匣子",它吸收各种要素投入并在预算约束下采取利润最大化行为。这种人格化的厂商观已经不能满足当前企业发展的需求,它过于简单,企业内部的很多关键问题都被忽略了,比如说信息不对称和激励问题,它也无法解释现代企业的很多行为。基于委托—代理关系产生的委托—代理理论深入到"黑匣子"中研究企业内部信息不对称和激励的问题,与交易成本理论等共同成为现代企业理论的组成部分。委托—代理关系被定义为一个人或一些人(委托人)委托其他人(代理人)根据委托人的利益从事某些活动并相应地授予代理人某些决策权的契约关系,显而易见,这种关系也存在于ICT外包业务中,因而委托—代理论主要用于ICT外包决策的成本考虑中。由于ICT外包的复杂性,许多学者试图从委托—代理论来构建ICT外包的决策模型。由于代理方与委托方的目标存在诸多不一致,代理成本是委托方进行外包决策分析所要考虑的重要方面,也是构建决策模型时,被格外关注的部分。

7. 价值链理论

价值链理论是由迈克尔·波特(Michael Porter)提出的。1985年迈克尔·波特在其《竞争优势》一书中提出了价值链概念。波特认为"每一个企业都是用来进行设计、生产、营销、交货以及对产品起辅助作用的各种活动的集合。所有这些活动都可以用价值链表示出来。"价值链理论认为,价值链的各环节互相联系、互相影响,一个环节的运行质量直接影响到其他环节,并对价值链整体造成致命损伤,对价值体系产生很大影响。因此,通过对企业的业务流程进行分析,找出企业价值链中的增值环节和非增值环节,从而便于企业对业务流程进行重组。将价值链上创造价值较少的活动外包给外部服务商,由外包服务商来提高外包活动的价值。企业通过外包,实行价值链的虚拟整合,可形成企业间的优势互补,从根本上提高价值链活动的质量。由于将本企业价值链的劣势环节用其他企业价值链中高效率和有比较优势的环节来代替,这实际上是价值链之间彼此环节中以长代短的虚拟整合,因而可形成价值链间的比较优势组合。简言之,从价值链理论看,资源外包能使企业资源更加专业化的集中到企业价值链的战略环节,与外包商形成优势互补,节约成本,并带来更大的灵活性[V1992]。

9.2.4 ICT外包发展

1989 年柯达公司把信息技术(Information Technology,IT)部门卖给 IBM,开创了巨型公司 ICT 部门外包的先河。同一年,拥有 130 亿美元资产的英国石油勘探公司(British Petroleum)开始考察 ICT 外包的可行性,发现外包本身是极为复杂和庞大的任务。经过相当长时间的研究,他们制定了行之有效的外包策略:设法使用多家(3 家)软件服务商,但又要求各家协作如一。五年后,他们成功地将 ICT 部门从 1400 人削减到 150 人,把相当于 1200 多人的 ICT 业务量外包给软件服务商,公司自身则集中精力改善核心业务流程,提高业务质量、削减运行成本,获得了良好的效益。从此,外包成为 ICT 产业发展不可或缺的一部分。

因经济发展和技术进步的程度差异,不同时期的 ICT 外包研究主题不尽相同。有学者从管理实践角度进行研究。认为 ICT 外包的动因既包括 ICT 外包所能为企业带来的收益、又包括企业所面临的各种压力,同时也体现了企业的战略意图。归纳起来,主要有以下几种动因,如表 9-1 所示[K2010]。

表 9-1 ICT 外包动因

外包动因	解释	主要文献
降低成本	承包商具备规模经济,能够提供低成本 ICT 服务	[CGJ1995]、[C2003]、[W1997]、[FR1995]、[KM2000]
聚焦核心竞争力	外包非核心 ICT 活动,聚焦发展企业的核心竞争力	[CGJ1995]、[W1997]、[FR1995]、[KM2000]、[LW1998]、[C2003]
ICT 能力因素	使企业获取内部无法获得的 ICT 服务	[CGJ995]、[W1997]、[FR1995]、[KM2000]
其他因素	现金需求、环境因素等	[W1997]、[FR1995]

(1) 企业进行 ICT 外包最为常见的动因是降低成本。企业普遍认为外部的承包商由于其规模经济优势、更加专业化的 ICT 管理技能、更易获取低成本劳动力等原因,能够以更低的价格提供与公司内部相同水平的服务。

(2) 企业进行 ICT 外包的另一大动因是聚焦核心竞争力。企业可以通过 ICT 外包将企业非核心的活动剥离出去,从而集中精力发展企业的核心业务,提高企业的核心竞争力。

(3) ICT 能力因素也是企业进行 ICT 外包的原因之一。企业通过外包获取先进的 ICT 技术。弥补企业内部 ICT 能力的“缺口”。

以上 3 点为企业进行外包最主要的动因,除此之外,还包括诸如企业通过外包 ICT 资产获取现金、企业内部的组织矛盾以及各种环境因素的原因等。

20 世纪 90 年代以来 ICT 的飞速发展赋予 ICT 服务商不断提升服务能力的可能,一种新的基于网络的计算能力实现了信息集中处理与存储的管理模式,使得用户通过简单的终端即可实现信息的访问与获取,IT 外包市场出现了一种新的 ICT 外包模式——ASP(Application Services Providers,应用服务提供商)。ASP 是指通过网络以一对多的方式

向客户提供标准化的应用软件、相关管理及咨询的租赁服务模式，托马斯·科恩等把ASP这种依托网络面向客户提供产品与服务的外包模式称之为网络外包(Netsourcing)，认为这是一种提供面向企业业务的服务的全新交付机制，是一种业务租用或“按用付费”，能够实现业务应用的集中管理。如果说ASP的出现为ICT外包增添了的新型服务交付模式，那么BPO(Business Process Outsourcing，业务流程外包)则是与客户组织业务密不可分的、高度相关的ICT外包模式。Gartner将BPO定义为一个ICT赋能的业务流程委托给第三方，它按照一整套定义好的方法来拥有、管理和操作业务流程。BPO区别于传统ICT外包的主要特点在于，外包商控制了与业务流程、人力资源和技术等相关的所有层面，是一种更为先进的ICT外包模式。随着ASP、BPO等新兴ICT外包模式的出现与发展，ICT外包的范围、程度在逐渐扩展延伸，其模式呈现多元化特点[C2011]。

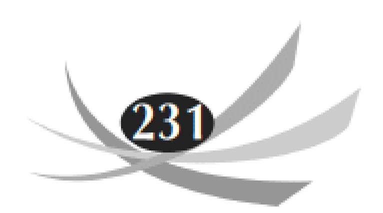
9.3 ICT外包安全模型

在对ICT外包特点的探索性研究取得相当多的一致性认识后，如何构建系统的ICT外包概念模型成为学者们研究的热点。外包模型是ICT外包研究的一个重要方面。ICT外包模型侧重于研究委托方与ICT外包商的关系方面，众多的学者从这个角度出发对ICT外包进行了研究。Kichan和Rajagopalan等根据外包信息系统的战略影响和外包度这两个维度把外包商关系分为信赖关系、战略联盟、支持关系(Support)和合作关系(Alignment)，通过实证分析发现，外包信息系统的战略影响主要表现为“成本节约”(Cost reduction)和“差异化”(Differentiation)两个方面。并且他们证明影响这两个方面的因素同时也影响与外包商的关系。Kiehan和Rajagopalan还发现只要以上两个维度有且仅有一个维度值为高的时候，对应的关系倾向于加强。Kishore则对四种关系进行深入的研究，对这四种关系的建立、维护所必需的能力、机制进行分析，同时还对这四种关系的演化进行分析。在与外包商的合同方面，Williamson根据市场方式与官僚方式在治理结构中的地位把合同分为经典合同、新经典合同和关系合同，对应这三种合同有四种治理结构：市场模式、三方模式、双方模式和官僚模式。Fitzgerald从合同定价方式出发，把合同分成六类：基于时间和材料的合同，基于固定费用的合同，固定费用加变动费用合同，成本加成合同，费用加激励计划合同和损益共享合同。Willeocks和Lacity对导致ICT外包合同失败的因素进行归纳。Jeffrey对多个竞标者参与的ICT外包合同如何达到最优化进行分析。De Looff提出一个IS决策的描述性框架。并用实证的方式对此框架的正确性进行证明。而Benko则强调ICT评估的重要性，提出应该按照建立当前ICT运行模型、评价ICT职能的战略目的、评价外包和自制这个三个阶段来对是否外包做出评估[QL2009]。

9.3.1 美国审计署ICT风险管理模型

随着ICT技术的日益发展，许多学者和专家也对这一领域展开了深入的研究，在此背景下，许多风险评估和风险管理模型应运而生。以下列举较为常用的几种模型。

第一个模型是美国审计署(US Government Accounting Office，US GAO)于1999年



发布的 ICT 风险管理模型，如图 9-2 所示。

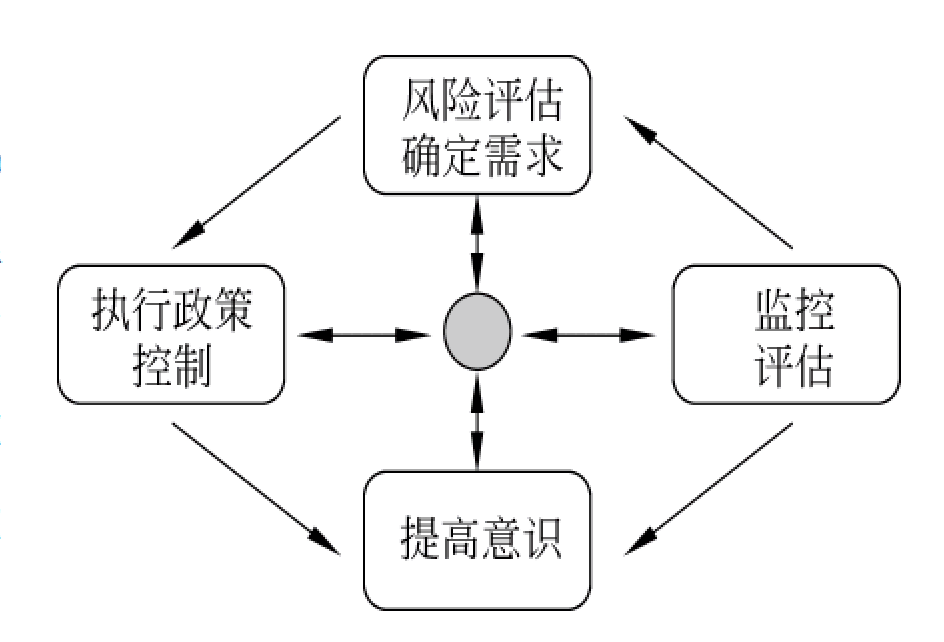


图 9-2　GAO ICT 风险管理模型

风险评估包括两部分，一是识别可能的风险；一是在相适应的情况使用对应的风险管理方法。发现风险后，采用实现规定好的规则和控制进行处理，同时提高对同类风险的预知能力。将预知和处理融入风险管理中，以此降低风险带来的影响。

在该模型中，风险管理的实施办法为建立一个中心处理节点，该节点负责执行对应的规则和相关的控制，提高预知能力，管理和评估规则和控制的效率[L2005]。

9.3.2 KPMG2 ICT 风险管理框架

第二个模型由 KPMG 组织提出，该模型以“风险成熟度框架”的形式出现。在它的组成部分中，活动和元素与之前提到的 GAO 模型类似。两个模型都包含活动和风险决断，然后对其进行测评和监控，并进一步采取相应的控制措施。风险计划或决策层包含整个框架的策略，框架如图 9-3 所示。

KPMG2 ICT(ICT)风险管理框架	
1	风险战略
2	风险结构
3	风险管理和指导
4	风险组合管理
5	风险消减和优化

图 9-3　KPMG2 ICT(ICT)风险管理框架

框架中的每一层都会包含如下策略中的一部分：

- 联系和管理组织经营战略的风险策略。
- 对风险策略起支撑作用的风险结构。
- 起到标准作用的测量和检测措施。
- 识别、评估、计量风险。
- 平衡风险容忍和潜在风险的能力。

这两种模型都采取了相似的风险管理方法，其关键就在于提供一个监控和测量核心，采用风险管理模型核心的特殊的标准。KPMG 模型延展了“行动”部分，它提出了应对风险的三种反应类型，即反应活动、设计和策略[L2005]。

9.3.3 ICT 外包决策三维模型

进行 ICT 外包决策时，一个较好的思考框架就是首先明确外包方案的选择(与外包服务商签订购入合同、付费服务合同、具有优先权的供应商合同、具有优先权的合同方/战

略联盟，和战略伙伴/联营企业等五种不同方案），然后考虑关键业务、成本和技术等影响外包决策有效性的各类因素。

1. 业务规则［WYH2006］

成功的外包首先要分析各种业务对公司的商业贡献。在图 9-4 中，Willcocks 从两方面——业务活动能对公司业务运营做的贡献和对竞争地位的影响，进行 ICT 外包决策。

对各种外包方案的选择应该是一个灵活的、动态的过程。一种关键的业务，随着运营和技术的改进，它的标准化程度会越来越高，该业务可能会转化为有用的业务。

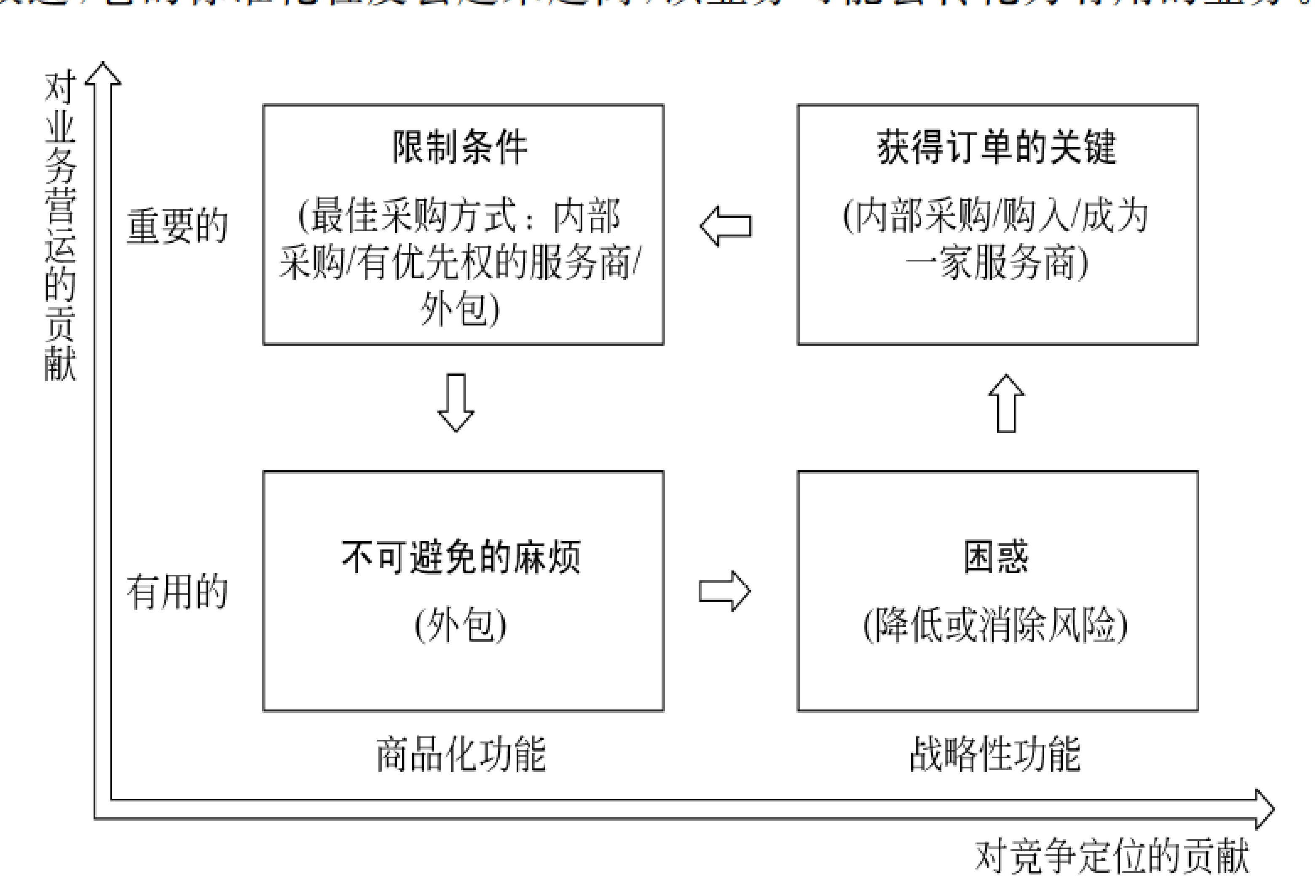


图 9-4 根据业务事项所作的战略化 ICT 采购分析

2. 成本因素［WYH2006］

成本方面需要考虑的因素较多，将成本与能力作为它的两个维度，同时分析市场与内部的成本和能力 Willcocks 认为，两个经济方面的因素，内部规模经济和采用先进的管理经验，将指导我们思考 ICT 外包服务商是否能够帮助我们减少成本，如图 9-5 所示。

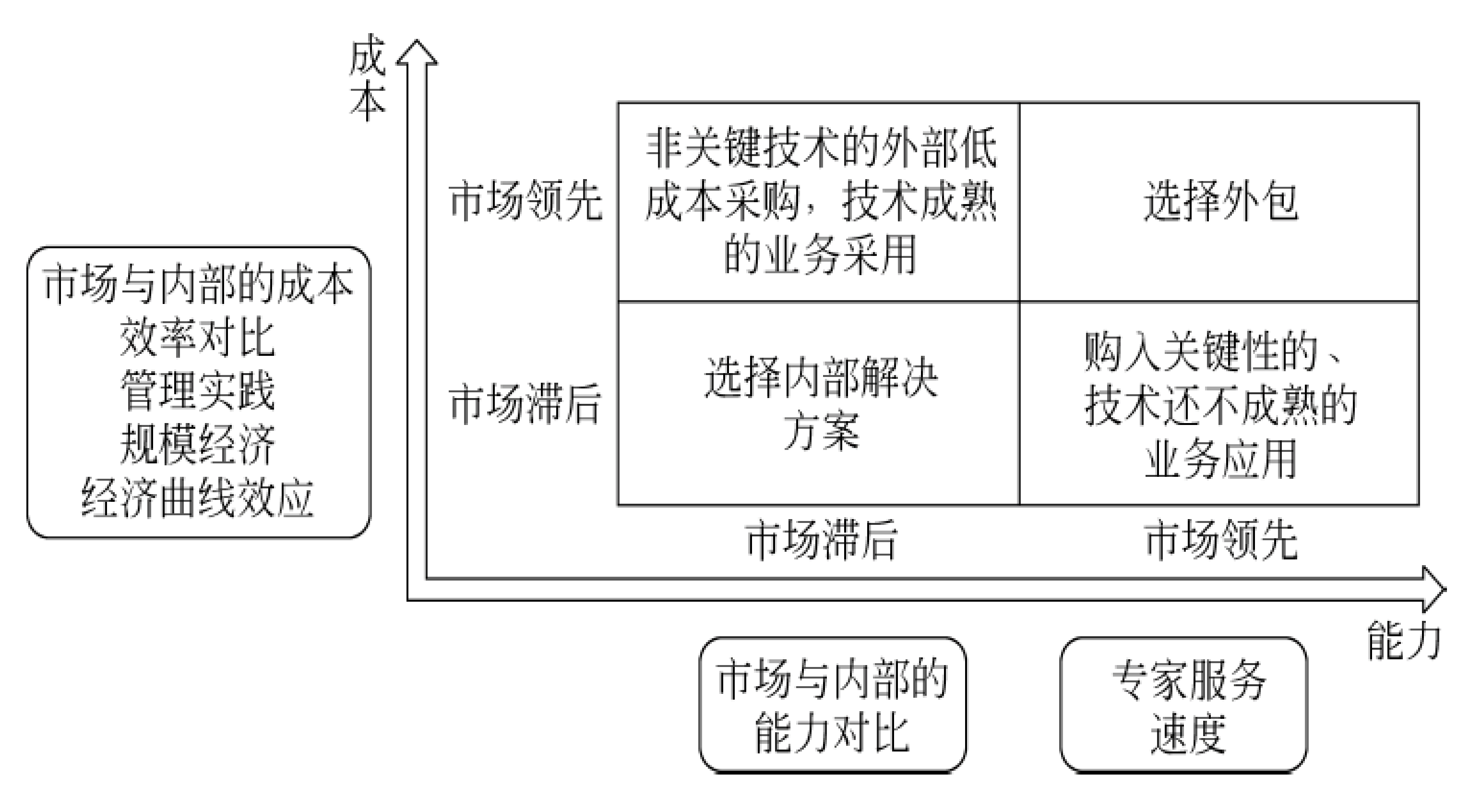


图 9-5 ICT 外包战略的市场比较

3. 技术因素［WYH2006］

对于技术方面，可以将技术成熟度和整合程度作为它的两个维度，建立模型，如图 9-6 所示。

综合以上分析，以关键业务为主线(因为它对企业的核心竞争力有着直接性的影响)，建立 ICT 外包决策三维模型，如图 9-7 所示。

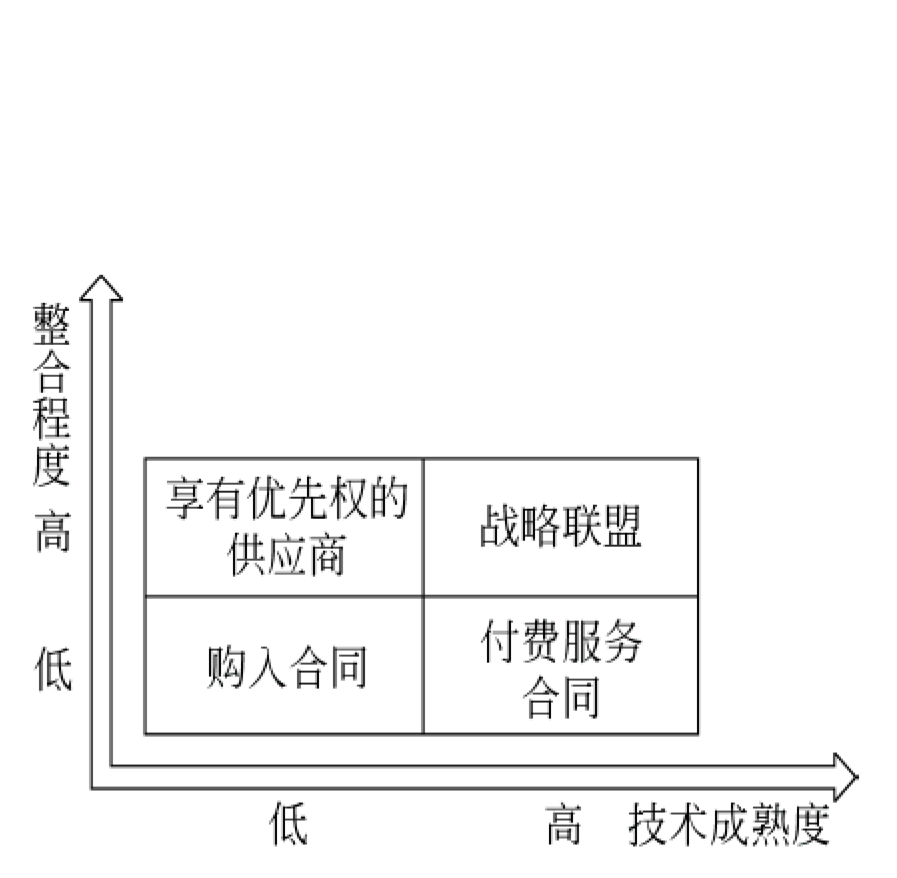




图 9-6 战略分析 ICT 外包：技术因素矩阵

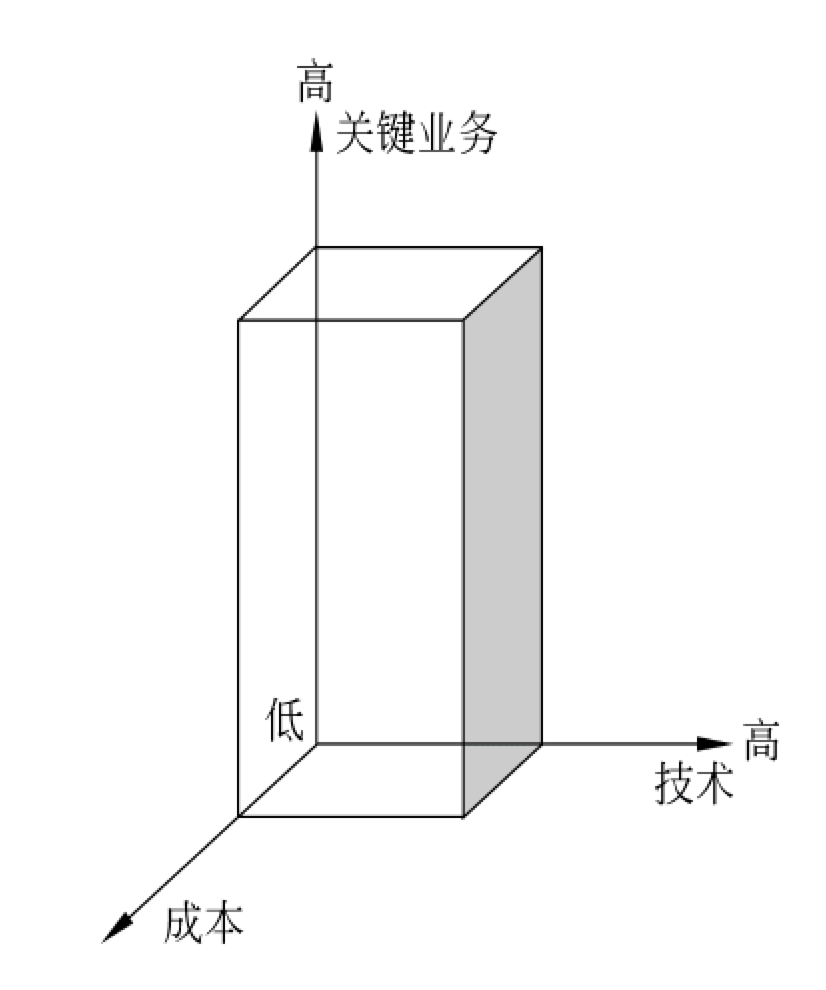


图 9-7 ICT 外包决策三维模型[WYH2006]

9.4 ICT 外包风险

虽然外包有很多优点，但企业将业务外包后，随着外界环境、市场的变化，以及人为因素，企业内部管理风险的能力等各种因素的影响，企业外包业面临着各种各样的风险，如表 9-2 所示。

表 9-2 安全服务提供商 SWOT 分析

	业务重点	优势	弱点	机会	威胁
IT 服务商	对高端用户的全面的行业解决方法	品牌优势资金雄厚	缺乏安全专业服务	提供全方位 IT 服务解决方案	恶性低价竞争
安全产品生产商	以安全产品市场为基础	核心技术专业服务	资金实力较弱	重点向中小型企业发展	竞争对手数量增多
通讯设备制造商	电信、金融、政府等市场	品牌优势网络基础资源资金雄厚	缺乏安全专业服务能力	重点向电信金融和政府等高端客户发展	较强的政策影响作用力
电信运营商	政府及其企事业单位	品牌优势网络基础资源资金雄厚	缺乏安全专业服务能力	与其他 MSSP 合作为中小企业服务实现双赢	与 MSSP 合作中的风险，客户流失

9.4.1 ICT 风险因素识别

ICT 外包风险因素分析就是运用风险识别方法来寻找出 ICT 外包过程中的风险因素。所谓风险识别就是采取有严格计划的步骤，在妨碍项目成功的因素变成问题之前发现并定位它们。风险如果不能被识别，它就不能被控制、转移或者管理。因此，它是企业

ICT 外包整个风险管理工作的基础。在这个过程中,外包企业要将 ICT 外包活动面临的各种不确定因素,也就是风险因素一一鉴别出来,并对关键的风险因素进行控制。ICT 外包的风险识别过程需要对企业自身的经营状况、战略目标、市场上服务商的数量及其 ICT 服务能力和其所处法律、社会、政治和文化环境有深入的认识,同时要求企业要有明确的经营战略和外包目标,由此方可识别促使外包成功的因素,以及那些威胁到企业战略目标实现的因素。此外,风险的识别还是一个动态的过程,随企业的外包需求、服务商的执行情况和其所在环境的发展变化而变化,贯穿于风险管理整个过程[BS7799 1993]。

在分析各个阶段的风险因素时,运用交易费用理论的两个重要假设来分析风险因素的来源。

交易费用又叫交易成本,是美国芝加哥大学教授科斯(Coase)在其《企业的性质》文章中首先提出的,是一种研究业务外包的常用理论。自科斯之后,威廉姆斯(Williamson)对交易费用理论做了较系统的完善。他在解释纵向一体化的分析框架中有两个重要假设,即有限理性假设和机会主义假设。有限理性假设指的是由于环境的不确定性和人类头脑本身认知的限制,使得充分估计所有可能决策的结果变得困难。例如,有限理性的程度部分依赖于外包企业详细说明其外包需求、选择适当的服务商和管理控制服务商等所需的知识和获取的信息。交易费用机会主义假设则指参与交易进行的各方,为寻求自我利益而采取欺诈的手法,同时增加彼此不信任与怀疑,因而导致交易过程监督成本的增加而降低经济效益。

在 ICT 外包关系中,由于服务商和企业之间的信息不对称,服务提供商可能会对企业隐瞒或编造一些不利于外包企业的信息,致使在外包企业选择服务商以及监督管理外包的过程中产生额外的交易费用,从而使外包成本增加,这将降低企业对外包的满意度。下面笔者将从交易费用理论的有限理性假设和机会主义假设这两个重要假设的角度来分析 ICT 外包各阶段的风险因素[NAN2010]。

9.4.2 决策阶段风险因素

在外包决策阶段,企业要做出是否外包以及外包什么的决策,评估及选择合适的服务商,为下一阶段的继续进行奠定基础。

1. 企业对核心能力的认识不足

核心能力是企业区别于竞争对手的持久地竞争能力,是企业持续竞争优势的来源。对于企业外包来说,通常不会把核心业务外包出去,对于某些非核心业务则可以选择外包。企业的核心能力可以有多种表现,例如专用性资产、组织结构、企业文化等等,因此对企业核心能力的识别是非常复杂的。企业核心能力的识别有利于企业核心业务的开展,把一些非核心业务外包出去,有利、有弊,如果企业外包决策者不能有效地识别出本企业的核心能力及核心业务,就不能确定正确的 ICT 外包对象。一旦将关系着企业命脉的核心业务外包出去,则存在失控的风险,而这种风险事件产生的损失则是巨大的,对企业的打击也是非常严重的。企业要做到规避风险,才能使各方面利益达到最大化。而要识别企业的核心能力还必须认识其三大特征。

(1) 知识特征。知识可以分为两大类:显性知识和隐性知识,具有信息特征的显性知

识很容易被仿制，而具有方法论特征的隐性知识则相对来说较难仿。核心能力必须以隐性知识为主，才能防止被仿制和替代。它可以被认为是关于如何协调企业各种资源用途的知识形式。

（2）资产特征。专用性资产对企业核心能力的投资是不可还原性投资，因此核心能力可以看作是企业的一种专门资产，具有“资产专用性”的特征。

（3）价值特征。创造独特价值核心能力的价值特征表现在三个方面：一是核心能力在企业创造价值和降低成本方面具有核心地位，核心能力应当能显著提高企业的运营效率。二是核心能力能实现顾客所特别注重的价值，一项能力之所以是核心的，它给消费者带来的好处应是关键的。三是核心能力是企业异于竞争对手的原因，也是企业比竞争对手做得更好的原因。因此核心能力对企业、顾客具有独特的价值，对企业赢得和保持竞争优势具有特殊的贡献。

针对企业核心能力的三大特征，可以从企业内部和外部来识别其核心能力。

（1）内部识别核心能力。

- 资产分析。企业内的专用性资产是获取和维持准资金的源泉。其中，由于巨额固定资产等有形的专用性资产所产生的优势容易被外界模仿而难以持久，因此稳定而持久的竞争优势主要来自于无形资产的专用性投资。无形资产中包括市场资产、知识产权资产、人力资产和基础结构资产。
- 价值链分析。价值链能有效分析所在企业所从事的所有活动中那些对企业获取竞争优势起关键性作用的活动，并说明如何将一系列活动组成体系以建立竞争优势。真正的核心能力是关键的价值增值活动，这些价值增值活动能以比竞争者更低的成本进行，正是这些独特的持续性活动构成了公司真正的核心能力。
- 技能分析。大多数竞争优势源泉根植于企业突出的技能，没有一个企业能在各种职能上拥有出众的技能，但成功的业务必定是源于某些职能上特定的技能优势。
- 知识分析。从知识的角度来识别企业核心能力，可以通过两种方法：一种是价值链知识分析，即在确认关键的价值活动后识别支持这些活动的关键知识，同一种关键知识可以支持几种关键价值活动；另一种是知识链价值分析，即从知识的吸收与传播、内化与外化、灌输与扩展等知识流过程出发来识别企业中具有特殊价值的知识，进而识别核心能力。

（2）外部识别核心能力。

- 竞争差异性分析。一个企业的竞争优势取决于所选择产业的吸引力和既定产业内的战略定位。即企业一方面应有能够进入具有吸引力的产业的资源和能力，另一方面应拥有不同于竞争对手能形成竞争优势的战略性资产。
- 顾客贡献分析。即分析在带给顾客的价值中哪些是顾客所看重的核心价值，弄清顾客愿意购买的究竟是什么；顾客为什么愿意为某些产品或服务支付更多的钱，哪些价值因素对顾客最为重要。

2. 不恰当的外包目标

企业希望通过ICT外包达到什么目的，也就是ICT外包的目标，是企业进行外包的动因，它是衡量企业外包成功与否的重要因素。因此企业ICT外包不恰当的目标成为

ICT 外包中隐藏的重大的风险因素之一。企业不恰当的外包目标总的来说可以分为三类：目标不明确、目标短视以及不切实际的目标。由于有限理性的存在，企业决策者如果不能很好的评估企业的优劣势，或者仅仅是在外包盛行的大环境下跟风而行，就无法明确企业究竟想通过外包得到什么，或是无法把目标通过详细的需求以说明书的形式来传递给服务商。在没有明确的目标的指导下，服务商可能根本就无法来进行具体的外包服务，而外包企业也无法以有效的标准对外包工作进行监督和管理。

3. 企业保留的 ICT 能力不足

企业将信息技术职能外包可以弥补企业信息技术能力不足，但是往往企业会过分的倚靠外包所带来的 ICT 服务而忽视了自己所应该拥有的业务。这就逐步加大了企业对外包商的依赖性，加大企业发展受限于外包商的风险，也可能使企业内部 ICT 部门的创新能力下降，以致影响到整个 ICT 部门的效率。而这些绝非是企业采用外包的初衷。企业内部保有恰当的资源可以更好管理和调动服务提供商，从而控制企业的 ICT 能力。因此企业在外包 ICT 业务的同时，也要使内部保有恰当的 ICT 能力。

4. 逆向选择

逆向选择是指信息不对称所造成市场资源配置扭曲的现象。在市场交易关系中，交易双方之间信息不对称是普遍的特征。当信息不对称发生在签约之前，逆向选择问题就出现了。在 ICT 外包中，由于信息的不对称和信息的不完全，企业缺乏服务商服务成本及服务质量的相关信息，而服务商对自己的了解远远比外包企业要多，拥有大量的隐藏信息。而在机会主义的驱使下，为了获得 ICT 外包合同，服务商可能会主观故意的提供不充分或不真实的信息，从而产生逆向选择问题。企业选择将 ICT 外包，正是看中了服务商在规模经济、经验以及对新技术的掌握等方面给企业带来的利益，因此选择一个适当的服务提供商对于 ICT 外包取得成功非常重要。一旦选择的服务商不能满足企业 ICT 外包的目标，导致中途更换服务商或是终止外包，都会对企业 ICT 外包活动乃至于企业整个组织带来严重的损失。因此，企业如何设计合理的契约菜单，以找到适合自己的服务商，成为 ICT 外包的关键环节。

5. 少量供应商

少量供应商(Small number of suppliers)指的是可供委托方选择的、能满足其需求的、著名的和值得信赖的供应商。在某一 ICT 服务市场上，如果可以满足外包企业需求的服务提供商很少，市场则缺乏公平的、有效的竞争，这势必导致企业各种成本的增加，其中包括：供应商的搜寻成本与签订合约的成本增加，而这些成本平均达到 ICT 外包总成本的 3%(Barthelemy, 2001)。根据迈克尔·波特(1985)的五力模型，供应商的价格谈判实力会受到多种因素的影响。当供应商产业由几个公司支配，且其集中化的程度比客户产业高，那么供应商往往能够在价格、质量及交货期上施加相当的影响。在这种情况下，企业与供应商的谈判成本就会增加。由于市场上供应商数量较少，企业一旦选定了某个供应商并形成大量的专用性资产，也会增加企业的转换成本，并进一步导致企业对服务供应商的依赖，而被供应商套牢(hold-up)。

9.4.3 执行阶段的风险因素

在外包执行阶段里,企业要与服务供应商签订一份详细又灵活的外包合同,来表述企业 ICT 外包的各项内容,并监督服务提供商按照合同的内容来完成整个的外包内容,同时以一定的绩效评价指标来衡量服务商的服务水平。

1. ICT 外包合同不完善

企业所面临的经营环境充满了各种不确定性,企业不可能搜集到所有与外包合同相关的可能发生的信息,或者搜寻这些信息需要很大的成本。因此企业也无法与服务提供商就所有可能出现的问题进行谈判并把它们写入到合同条款中,导致了外包合同的不完善,这是 ICT 外包结果不能达到企业需求的重要的因素之一。合同的不完善导致企业与服务商不能通过合同来明确双方的权力、义务,那么,就无法有效地约束当事双方的行为,结果双方都会为单方面追求自己的利益而损害对方的利益。

2. ICT 外包合同缺乏灵活性

企业与服务商的合同尤其是长期的外包合同,除了要具备完善的条款还要有一定的灵活性,以应付 ICT 的发展、外包活动操作方面的改革甚至企业战略目标的变化。如果合同的内容仅仅着眼于短期的企业发展和技术更新,那么一旦企业的外包需求发生变化或 ICT 技术出现了历史性的革新,合同没有相应弹性条款来应对这种情况,则会将企业限制在合同的范围里,导致外包中断的风险。同时,外包合同通常是中长期的,外包时间越长,企业对服务商的依赖越大,僵死的条款、缺乏应急条款、缺乏谈判机制等都可能导致合同自身缺乏灵活性,这样的合同往往在情况发生变化时给企业造成不良后果。

3. 企业与服务供应商之间的沟通不畅

企业与服务商的合作是一个长期的过程,需要双方经常进行信息交流,通过沟通及时发现并解决问题。当内部的 ICT 业务或资源交由外部的服务商管理之后,企业无法对外包的内容进行直接控制,因此,企业应该积极地与服务供应商进行沟通,对服务商的管理进度以及服务质量有所了解,通过沟通及时发现并解决问题,这就要求建立健全信息化管理体系。然而信息化管理体系的推广实施,往往又容易被忽视。消极的逃避沟通或与服务商的沟通不畅都会大大的助长其机会主义的产生,从而导致 ICT 职能失控、服务质量的下降等结果。

4. 服务提供商的 ICT 技能不足

企业之所以选择 ICT 外包,就是希望将自己不擅长的业务交给专业服务商去做,从而达到专注核心业务、节约成本等目的。而企业一旦选择了 ICT 外包,服务商的 ICT 能力对于外包的成功起着决定性的作用。但是由于服务商的能力有限或是与外包企业所期望的实力存在差距,则势必会给企业的外包带来巨大的风险。

5. 企业监控不力

当企业将部分 ICT 资产和人员交由外部服务商管理时,企业就不能像以往在企业内部一样对这些资产的运行进行监控。企业缺乏对服务商有力的监控会导致外包项目的进度以及完成的质量得不到有效的控制并且也无法进行及时的修正而且有可能促使服务商机会主义的产生。服务供应商很有可能不履行先前的合约承诺,不考虑企业的外包利

益，降低外包质量。另外，企业在将 ICT 业务外包的同时，也不得不将公司经营的相关信息告知服务商。但是，服务商并非只为一家企业提供 ICT 外包服务，在掌握了众多客户的信息资源后，服务商有可能会把有价值的信息透露给企业的竞争对手，企业商业机密的丧失会使企业在市场竞争中失掉先机，给企业的经营带来巨大风险。

6. 缺乏有效的绩效评估指标

外包成功被定义为“组织对通过采取外包战略所获得的利益感到满意”。通常认为，外包成功的标志是客户组织得到了满意的结果。然而“满意”只是人主观上的一种感觉，只有把它转化可见的评估指标才能够更好的评估服务商提供的 ICT 服务质量。一般情况下，对供应商服务水平的评估是基于合约条款，而合约条款多数只对结果做出描述，因此对外包业务过程不能进行有效的评估，无法衡量外包活动的成功与否，也不能建立适宜的持续改进机制。随着时间的推移，当企业准备向供应商增加外包项目时，才发现供应商已不符合企业进一步发展的要求[E1996]。

9.4.4 ICT风险应对方法

(1) 风险预防：风险预防就是事先估计风险产生的可能程度，判断导致其出现的条件和因素，力求从根本上消除风险的影响。任何事物都有风险，ICT 风险归根结底，也是可以通过一定手段和有效措施加以预防的。通过制定策略规划，制定严格的规章制度，用标准化、制度化、规范化的方式从事项目的相关工作，可以避免可能引发的风险或不必要的损失。这种预防风险方法通常称为程序法，是一种十分有效的风险规避方法。另外还可以采用教育法来预防风险，所谓教育法就是对项目成员进行教育培训，提高项目成员的风险意识和及辨识风险的能力。

(2) 风险回避：风险回避是指将风险行为减到零，是回避风险最直接和有效的方法，当项目风险潜在发生威胁的可能性太大，不利后果太严重而又无策略可用时，为了不让项目给业主带来不能控制的风险，从而主动放弃项目或者改变项目目标与行动方案。选择回避项目是最简单的回避风险的方法。但这也是一种消极的手段，而且随着项目进程的推动，风险回避所付出的代价将越来越昂贵。

(3) 风险转移：风险在卖方尚未将货物交付承运人或买方前、在运输途中及买方在收到货物后等各种情况下都可能发生。风险的时间如何计算，货损的责任由谁来承担，切实关系到买卖双方当事人的切身利益，也因此而成为货物买卖中一个复杂而重要的问题，即风险转移问题。风险转移是设法将某风险的结果连同对风险应对的权利和责任转移给他方。一般来讲，风险转移分为保险和非保险两种方式。ICT 外包项目一般同时采用两种风险转移方式：比如引入信息化咨询与信息化项目监理，降低项目中可能出现的风险；引入硬件设备维保服务商，提升运营效率和降低备件费用，消除项目中不可控的风险。

(4) 风险自留：又称风险承担，是指对一些无法避免和转移的风险采取现实态度，企业自己主动承担风险，即指一个企业以其内部的资源来弥补损失。风险自留与其他风险对策的根本区别在于：它不改变项目风险的客观性质，即既不改变项目风险的发生概率，也不改变项目风险潜在损失的严重性。风险自留要求对风险要有充分的认识，同时必须制定后备措施。

(5) 风险后备：这是一种风险损失控制的方法，通过实现控制和应急方案使得风险不发生或者发生后的损失额最小。损失控制分为预控方案和应急方案。预控方案是通过主动控制风险发生的条件使得风险不发生；应急方案是使项目风险损失最小化，在损失发生时起作用[ZZH2008]。

9.5 ICT外包管理

9.5.1 ICT外包管理对企业ICT绩效的影响

如果说ICT外包战略决策内容对企业ICT绩效有着重要影响，那么ICT外包执行过程的管理则是企业ICT绩效实现的关键。

管理是在有限的资源约束条件下，通过组织的共同努力，运用各种理论和方法，对本身进行计划、指挥、协调与控制以实现的制定的目标，管理是基于协作的策略。而项目外包是通过跨企业的业务，将各个企业联合在一起，实现整个供应链。通过对供应链整体运营状况和节点企业之间的运营关系进行管理，可以了解运营状况，对绩效不高的管理做出相应的反馈和调整，优化企业运作流程，使之发挥最大效益。

项目外包管理是企业用于实现企业外部管理的手段，如果没有采取恰当的管理方式，整个供应链可能都将会受到影响。对于ICT外包管理的实施，可以从以下方面进行：

(1) 集成的管理体系。Internet的问世，电子商务的产生，供应链管理和管理思想的集成，这些都显示出社会发展的网络化、整合化、电子化、客户化、协作化的一种趋势。对一个项目的实施，对一件产品的生产不再仅仅是某个企业独立完成局限在企业内部了，而是由企业群之间进行联合设计、分布式生产，这些都促使管理体系进行拓展，实现管理体系思想的集成。

(2) 合作商的选择。在决定项目外包时，要选择合适的合作商，需要考察合作商的技术优势、财政状况等全面情况，同时咨询专家的意见，从而科学的选出符合自身要求的合作商。项目外包合同通常是在基于双赢的原则上建立的，并且要保证整个合同的顺利履行及对合作商的有效监督、评估和控制。

(3) 多方面管理。进行ICT外包管理时，对项目的各个方面都要及时掌控其运作情况。还要注重物流方案管理、信息技术管理、风险及绩效管理。

总之，项目ICT外包管理的关键是采用集成的管理思想和方法，把企业内外部有机的集成起来进行管理，形成集成化的管理体系。通过管理将企业生产经营过程中及各合作企业之间的物料流进行有效的控制和协调，风险得到规避和弱化，最终达到全局动态最优目标，以适应竞争环境下市场经济的要求[ISO 13335 1996-2001]。

9.5.2 ICT外包管理面临的挑战

传统的管理是以其九大知识领域为主要研究内容，以单或多项目的研究为中心，局限于单一企业内部环境下的运作模式。如果把项目进行分解并外包，项目的实施将跳出企业内部，必然涉及到相关战略合作伙伴企业间的协作和竞争，这将会对传统的管理模式提

出挑战。作为主体企业,如何改变自身的运作方式,加强自身的管理,使之适应新的社会发展模式,如何快速组建有效的战略合作满足各方面社会的约束,这些都是传统管理理论体系所无法解决的。如何对原有理论体系进行拓展,吐故纳新,汲取优秀的管理思想和理论体系来充实企业管理的理论框架,使之更好地服务于企业,这是ICT外包管理理论体系面临的重大挑战。

传统管理方式的特点是以目标为驱动,管理界面清晰,机制灵活,虽然在过去的实践中,传统管理模式已经大获成功。但随着供应链管理思想和项目外包的盛行,原有的这些成功因素已经不能完全满足管理的要求,ICT外包管理已经对传统的管理思想提出挑战,这种挑战主要来源于以下几个方面。

(1) 传统管理思想对管理提出的要求。作为传统的管理思想,要求管理界面清晰,它要求在一定的条件下,自己完成一定的任务即可,但现在管理变成嵌入式的,在很多地方需要相互配合,许多细节的工作在开始时是很难定义清楚到底是谁来负责。同时ICT外包管理要求一定以供应链上的企业群多赢的战略角度出发,这使得管理的难度加大,传统的管理模式难以适应。因此,ICT外包管理迫切需要一种能以多赢为出发点,根据客户需求,快速响应市场,充分发挥项目外包的优势,实现高效率、高度共享、高度集成的管理体系。

(2) 加强合作商的选择。目前企业在选择项目外包合作商时不能科学的做出评选,唯价格论就很能说明合作商有很强的随机性和盲目性。还有,单纯的任务供应合作商的公司规模越大越好,忽略企业文化的融合性,这样很容易产生不同企业文化的摩擦与撞击,导致项目外包关系的破裂。因此,ICT外包管理应在合作商选择时就已经开始运行,帮助企业选择最适合的合作商。

(3) 需要改变传统的物流管理。目前大多数企业的物资准备是按照种类,需求的量一次性到位的,这样不仅时常造成库存积压,还经常的使生产过程间断或拥挤,不但不能及时应付临时变更,而且造成了其他物料统筹混乱,给生产、物资部门均造成不必要的麻烦,而且响应不了市场需求。在财务上,也不利于物料的成本核算和控制,尤其是协作部门的利益核算、绩效考核。因此能够与区域导向的生产、设计充分结合的物流管理就成为十分有必要的事。

(4) 需要改变传统的信息化建设。计算机和信息技术这样的工具和手段将企业管理水平推上了一个新台阶,尤其是规模大的企业,要处理庞大的工作量,更需要完善企业的信息设备和管理系统。管理软件是管理系统的信息处理的集成化体现,它的应用是实现信息技术与管理模式接轨的重要手段和标志之一。管理软件使企业各部门及企业之间,信息沟通越来越方便。但目前,个别企业虽然上层信息系统建立起来了,但管理软件却没有得到充分的应用,这具体表现在基层和上层管理部门、企业和协作单位之间、企业和上下游企业之间的信息沟通不畅等方面。在ICT外包管理中,应注意这些问题,从而充分利用信息技术。

(5) 需要增强风险管理。业务外包风险来源非常广泛,企业自身,合作商,还有外包契约都有可能成为风险的来源。而且在项目实施的各个阶段,也都有可能产生风险。对于不同的阶段,风险影响因素也并不相同。外包决策阶段风险因素主要涉及外包企业的

有限理性、外包服务商的缺陷、外包交易的潜在依赖三个方面;而外包的实施阶段则主要涉及道德风险、成本失控及协调问题等方面。与此同时,在业务外包的实施阶段,不同的业务外包模式也意味着风险大小的不同。由于这些风险对业务外包的成功实施起着决定性的作用,企业必须增强风险管理,评估风险的级别并结合企业的可承受风险级别采用不同的控制策略,对不同的风险采用不同的防范措施。

(6) 需要加强绩效管理。从人力资源的角度看,实施绩效管理和绩效考核,很重要的作用就是通过绩效考核在组织内部制造差异,从而带来激励。也就是说,企业希望通过绩效管理的实施在组织内部制造差异,利用差异达到激励员工的目的。很多企业在没有取得绩效管理预期效果时,不是怀疑自己实施的方法是否有问题,而是开始怀疑绩效管理的作用,甚至很多企业认为绩效管理只适合大企业,不适合中小企业。这属于适合论、失败论。在ICT外包管理中,也应建立起绩效管理,从而通过这种方式对企业的战略目标、员工的阶段性工作目标进行管理和监控。

9.5.3 ICT风险管理系统

由于ICT外包存在着种种风险,因此建立系统化、制度化的动态的外包风险管理组织系统,对ICT外包风险监控管理及风险防范是十分必要的。从许多国际大企业的成功经验来看,他们均有成文的风险管理制度、有效的组织管理机制、良好的人力资源储备和具有风险意识的企业文化,这些都是特别值得ICT外包管理所借鉴的地方。

ICT外包风险管理组织系统主要由制度化的、系统化的有关不确定性管理的业务流程和风险管理组织机构组成。

由于企业业务流程不合理、不规范,缺乏ICT外包风险防范机制,从而导致ICT外包风险的产生。因此,企业应针对ICT外包可能产生的不确定性而带来风险进行业务流程重构(BPR)。这些基于风险防范的流程在业务正常时不起作用,但当不确定性发生时会及时启动并有效运转,并对不确定性风险导致的危机的处理发挥重要作用。如德勤咨询曾经协助北美一家大型汽车公司对90个业务流程进行风险相关分析,对其中的30个有可能发生的重大危险的至关重要的业务流程进行重新设计,使这些流程不仅能满足企业正常运作时的要求,而且能够承受可能因不确定性导致的一些重大危机,或者可以在危机时进行灾难快速恢复。

风险管理机构是风险识别、分析、评估、监控、防范、处置的运作主体,是风险管理工作的组织者与防范措施、方案的制定者,建立权责对等的企业风险管理机构将有利于物流外包风险管理的制度化、经常化。

企业风险管理机构的人员构成,原则上应有财务、法律、各业务单位的成员代表。机构规模的大小可根据机遇产品的生产规模、技术与生产经营过程复杂程度、营销难度和联盟成员企业(外包商)的多少,并对风险管理成本和利益(避免风险的损失)进行比较后来决定。外包风险管理机构的基本职责有:负责外包风险防范设计、检查、监控、预警和发布风险处理指令。负责建立和完善外包风险管理机制。负责企业合作开发、生产、销售、物流等信息的收集、查询、分析,并及时公布合作事项质量、进度、成本、交货期等各种信息。负责监督外包企业的履约情况和协调外包管理工作。负责外包例外风险的处理决策。负

责外包合同终止阶段的善后处理。

企业在进行组织设计、规章制度的制定时，应有风险管理人员参与，将风险防范机制引入企业各规章制度中，通过制度来规范外包过程，以制度来规避风险。

在风险管理组织建设中，风险突发应急机制的建立也是非常必要的，由于外包物流管理是多环节、多通道的一种复杂的系统，很容易发生一些突发事件。外包物流管理中，对突发事件的发生要有充分的准备。对于一些偶发但破坏性大的事件，可预先制订应变措施，制订应对突发事件的工作流程，成立应变事件的处理小组(合作双方或单方)以应对各种突发的严重性风险危机应急机制也是时分必要的，避免当严重风险突然发生时，茫然不知所措或做出错误的决定[MJ2010]。

9.5.4 管理与外包商的关系

管理好与外包商之间的关系，意味着服务采购方应致力于和外包商建立长期合作关系，这将有助于安全服务的外包商更多地了解用户的文化，从而提供更好的服务。传统的交易追求最大程度的节约成本，它与外包商的关系是比较单纯的买卖关系。这种关系主张把对外包商的依赖程度降到最低，把对外包商的讨价还价能力提高到最大。而随着业务外包的深入，外包企业所面对的供应商关系愈发复杂化。当全球竞争继续发展并且延伸到不同行业中，单纯的交易关系已无法满足企业的需求，企业应该在注重监督与控制的同时，同样注重对外包商的激励和协作。以建立良好的可发展的关系为关系管理的基础[SNA2008]。

参 考 文 献

[BS7799 1993] Val Thiagarajan. Code of Practice for Information Security. SANS，1993.

[ISO 13335 1996-2001] Guidelines for the Management of IT Security. GMITS，1998.

[E1996] Michael J. Earl. The Risks of Outsourcing IT. Sloan Management Review，1996.

[C2011] Christof Ebert. Global Software and IT A Guide to Distributed Development，Project，and Outsouring. IEEE computer society，2011.

[ML2009] Mary C. Lacity. Information Systems and Outsourcing. 2009.

[K2009] Kirk St. Amant. IT Outsourcing：Concepts，Methodologies，Tools，and Applications. Business science reference，2009.

[MAH2011] Taghavi. Web Base Project Management System for Development of ICT Project Outsourced by Iranian Government. International conference on Open Systems (ICOS) 2011 IEEE，2011.

[ZZH2008] Zhang Pei . A Framework for IT Outsourcing Decision Process. IEEE，2008.

[NAN2010] Nik Zulkarnaen Khidzir. Information Security Risk Factors：Critical Threats and Vulnerabilities in ICT Outsourcing. IEEE，2010.

[MJ2010] Michal Sebesta. On ICT Services Management and Outsourcing. 2010 2nd International Conference on Software Technology and Engineering(ICSTE)，2010.

[QL2009] QU Gang. Research on model of knowledge transfer in outsourced software projects. 2010

International Conference on E-Business and E-Government，2009.

[SNA2008] Syaripah Ruzaini Syed Aris. Risk Management Practices in IT Outsourcing Projects. IEEE，2008.

[W1997] Warren，David R. Defense Outsourcing：Challenges Facing DOD as ICT Attempts to Save Billions in Infrastructure Costs. General Accounting Office Washington Dc National Security And International A Ffairs Div，1997.

[FR1995] F. Warren McFarlan. How to Manage an ICT out-sourcing Alliance. Sloan Management Review/Winter，1995.

[KM2000] William R. King. Developing a Framework for Analyzing IS Sourcing. Information&Management，2000.

[LW1998] Lacity MC. An Empirical Investigation of Information System Sourcing Oractice，Lessons from the Experience. MIS Quarterly，1998.

[C2003] Currie，W. L. A Knowledge-based Risk Assessment Framework for Evaluating Web-enabled Application Outsourcing Projects. International Journal of Project Management，2003.

[B1991] Barney J. B. Fiml Resources and Sustained Competitive Advantage：A Rresource-based View. 1991.

[CGJ1995] Myun J Cheon. Theoretical Perspectives on the Outsourcing of Information Systems. Journal of Information Technology，1995.

[PH1990] C. K. Prahalad. The core competence of the corporation. Harvard Business Review，1990.

[V1992] Ravi Venkatesan. Strategic sourcing-to make or not to make. Harvard Business Review，1992.

[WYH2006] 王永红. 国内 IT 外包服务发展探讨与实例研究. 2006.

[LH1993] Lacity，M. Implementing Information Systems Outsourcing：Key Issues and Experiences of an Early Adopter. Journal of General Management，Vol. 19，1，1993：pp. 17-31.

[LV1992] Loh，L. Determinants of Information Technology Outsourcing：A Cross-Sectional Analysis. Journal of Management Information Systems，1992.

[RW1998] Robert Klepper. Outsourcing Information Technology，Systems，and Service. Business Forum，1998.

[K2010] Kirk St. Amant. IT Outsourcing Concept-Methodologies-Tool-and Applications. Business Science Reference，2010.

[L2005] Ian Tho. Managing the Risks of ICT Outsourcing. Butterworth-Heinemann Ltd，2005.

第10章 构建我国ICT供应链安全

10.1 概　　述

ICT产品历来都是非常敏感的问题,供应链安全问题实际早就存在,包括我国在内的世界各国都关注过这个问题,只是早期没有明确它的定义而已。

随着贸易全球化的发展,ICT产品的跨国流通越来越频繁。在产品从采购原料、生产、运输直至交付给最终客户的过程中,任何一个环节都有可能存在影响ICT产品的因素。如果考虑到信息安全的对抗性质,来自国外的ICT产品供应商完全有可能、有条件在产品中设置恶意功能。这就是ICT供应链的安全问题。安全可靠的ICT产品是信息安全系统的基础,因此,确保ICT产品供应链的安全,已成为加强信息系统安全保护的一项基础性工作。

供应链中参与的主题众多,产品从原材料采购,到交付时处在复杂的环境之中,使得供应链安全问题本身非常复杂。

美国掌握着世界上最先进的信息技术,其ICT企业在全球市场占据垄断和主导地位。美国将ICT产品的供应链安全作为加强其自身信息安全保护的重要考虑,其有关政策和措施值得我们认真思考。

美国首先将供应链安全作为问题提出。IBM公司在2003年9月12日发布的《供应链安全指南》中,系统的谈论了供应链安全问题。2006年,美国出台了《港口安全运输问题》法规,增强作为实体的供应链链条的强度。2007年,美国国土安全部发布的《增强供应链安全的国家战略》,针对供应链安全提出了31项对策,从政策、标准、机构、职责、法律以及具体执行都提出了一整套的办法。在这些基础上,产生了2008年1月8号布什总统的54号令,或者叫12点计划(英文简称CNCI),也就是国家网络空间综合保护计划。在这里面专门有一个问题讲述供应链的安全问题,此计划把供应链安全问题提到了一定的高度。

我国实际上也存在着大量的供应链安全问题,而且威胁相当严重。目前和国外相比,我们的问题要更加严峻。因为我国的很多核心技术,都不掌握在自己手里。在与ICT有关的技术中,我国做的更多的是应用部分,而基础软件如操作系统等,则并没有成型并得到大面积的推广。所以这个问题实际上很严重,但到目前为止,只是学术界和部分相关部门特别重视这个问题。而对于国外来说,这个问题早已进行了二十多年的研究和实践。

供应链安全现今正面临着严峻的挑战,全球供应链的安全不仅是各国政府,也是商业领域必须关注和直面的一个课题。自美国"9·11事件"后,美国国土安全部海关边境局



(CBP)就制定了海关-商业伙伴反恐计划(C-TPAT),开启并带动了全球供应链安全管理要求的实施和发展,使它逐渐成为一个全球性的普遍要求。中国在加入 WTO 以后,中国的企业面临着更加激烈、更加严峻的国际竞争形势,要想在这样的竞争环境中求得生存与发展,就有必要加强我国企业的供应链管理,提高供应链管理的水平,寻找在国际供应链中的准确落脚点,以此来提高我国企业在国际竞争中的力量。

10.2　我国 ICT 供应链的发展及相应问题

随着新世纪经济全球化的发展以及新技术的应用,跨国公司开始在全球范围内建立自己的供应链体系。发展中国家的产业能否参与到跨国公司的全球供应链体系中来,以及在这个体系中能否拥有自主地位,将决定这个国家能否掌握自身的经济命脉。同时,这也是发展中国家在国际分工中成功发展自己的关键。因此,作为发展中国家必须了解分析形势,把握发展趋势,认真研究政策导向,并积极应对。

10.2.1　我国 ICT供应链发展现状

供应链管理在我国的发展大致可分为以下几个阶段[LM2009]。

(1) 1978 年以前,我国的制造业相对比较落后,ICT 产业更是从零起步,企业对“供应链”这个概念几乎是一无所知。企业要生产什么,往往不是自己决定,而是被原材料推动的,ICT 产品的按需设计、用户反馈更是无从谈起。此时由于计划经济和短缺经济的大环境影响,企业拼命技改、抢项目、扩建厂房、更新设备,导致制造能力大量过剩,而销售和供应能力则很弱,形成典型的“腰鼓型”呆滞式企业,而在所生产的产品中,初级产品占的比例非常高,高端的通信电子产品仅用于军工产业。这个年代被称作供应链的“推式”时代。

(2) 1972—1992 年,中国的对外贸易蓬勃发展,在这个阶段,企业开始注意充分利用内部资源,客户的需求也逐渐成为影响企业经营活动的重要因素。在客户需求的“拉动”下,企业开始注意对整个经营活动加以控制和管理。随着改革开放的进行,众多国外 ICT 产业的先进技术与产品被引进国内,这段时间是中国信息产业开始全面奠定基础的时间。当时的中国对信息技术的应用几乎接近于空白,而作为 ICT 世界领航的美国在信息产业已经领先于中国近五十年的发展,并且在 20 世纪 90 年代初爆发的海湾战争中开始全面娴熟地运用信息战这样全新的作战模式。面对中国这样庞大的市场和如此反差鲜明的技术差距,中国一度成为全球信息产业过期产品的“抛售地”,很多公司将全球市场中没有消化的产品拿到了中国市场来进行销售。在这个阶段,中国更多客户奉行的不外乎是一味的“拿来主义”和“闭门造车”,当时在中国这个有着强大投资潜力和市场需求的主战场上曾经硝烟弥漫,国外公司虎视眈眈地准备开拓中国市场,又由于当时政策的限制,不得不和国内地方势力结合探询共同发展策略。这个阶段,是中国信息产业发展过程中不可逾越的时期,也是在这时,地方 ICT 企业开始了原始资本的积累,然而这个时期又充满着盲目和不确定因素的复杂环境。因此这些年又被称作供应链的“拉式”时代。

当时的技术以引用为主,单纯的“拿来主义”导致了许多问题的产生。首先,存在着管

理软件本身的技术问题。当时引进的国外软件大都运行在大、中型计算机上，多是相对封闭的专用系统，开放性、通用性极差，设备庞大，操作复杂，系统性能提升困难。而且国外的软件没有完成本地化的工作，再有就是耗资巨大又缺少相应配套的技术支持与服务等问题；其次，存在着缺少应用与实施的经验问题。再次，存在着思想认识上的障碍问题，当时企业的领导大都对此重视程度不够。故从整体来看，企业所得到的效益与巨大的投资及当初的宏图大略相去甚远。

(3) 1993 年以后，中国的经济体制逐步由计划经济转变为市场经济，市场逐步繁荣，大部分商品已呈现过剩，产品质量等因素在竞争中的优势逐步减少，本地竞争优势逐步体现出来。在这种情况下，企业不得不开始考虑如何从原材料采购开始就加以管理和控制，以提高企业的整体效益，从而在激烈的市场竞争中立于不败之地[PWC2011]。

然而，这仅仅是刚刚开始了供应链内部集成的阶段，中国对供应链的研究才刚刚起步。过去国内企业对供应链的关注主要集中在供应商制造商这一层面上，而这只是供应链上的一小段，研究的内容也局限于供应商的选择和定位、降低成本、控制质量、保证供应链的连续性和经济性等问题。因此，目前在我国企业界还没有形成真正意义上的供应链。就我国脱胎于计划经济模式的国有企业和中小规模的大量加工生产企业来说，供应链和供应链管理仍然是比较陌生的概念。

虽然提高顾客的满意度以及削弱成本的要求使人们对供应链的重要性的认识日益增加，但不可否认的是，中国 ICT 供应链还处在萌动的阶段。随着国内经济的快速发展以及全球化的不断增强，我国已经具备了发展供应链和物流管理的实力。企业的竞争力格局正在改变，生产企业和物流企业越来越多的使用供应链管理技术和现代科技手段，提升自己的核心竞争力。21 世纪的竞争，不仅是企业和企业之间的竞争，也是供应链和供应链之间的竞争[QJ2007]、[Y2011]。

10.2.2 我国 ICT 供应链发展趋势

ICT 供应链是动态系统，自从其出现以来就没有停止发展。只有把握住 ICT 供应链发展的要求、市场的变化及信息技术的不断发展这些发展趋势，才能提高供应链的敏捷性，降低运营成本，实现供应链的协同发展和整体利润最大化。

(1) 提高对供应链管理的认识。加强对供应链的管理在美国和欧洲开始于 20 世纪的 70、80 年代。我国的供应链管理的思想是 20 世纪 90 年代与现代物流一起引进的。经过十几年的努力，特别是近几年的实践，我国东南沿海的大型制造业和流通连锁企业的供应链管理已日趋成熟。例如家电制造业的“美的”、ICT 业领头羊“华为”已从供应链的整合和重组中获得了巨大的利润空间和竞争力。

(2) 对现有的供应链进行整合。实际上供应链对于制造业和流通业是早已存在的。现在的问题是如何认识它的重要性，对其进行优化整合，并通过现代信息技术加强对它的管理。对供应链的整合，主要是对业务流程的优化。不断加强其核心业务，将非核心业务外包。使企业内部供应链外化，特别是物流的外包，来提高企业的核心竞争力。如“华为”集中人力优势进行高科技的研发。整合供应链要对供应商和分销商进行优化选择、动态管理，使整个供应链对市场更具有快速反应能力，从整合中要效率和效益。

(3) 加速推广现代信息技术的应用。现代信息技术既是现代物流的基础，也是供应链管理的基础。信息共享是供应链管理的基点，加速推广现代信息技术的应用，将极大地促进我国 ICT 技术的发展[LM2009]。

10.2.3　我国信息化发展战略

2006 年 5 月，中共中央办公厅、国务院办公室印发了《2006—2020 年国家信息化发展战略》(以下简称《战略》)。《战略》颁布以来，引起了社会各界的广泛关注。国家信息化战略的编制和颁布是经济和社会发展的必然要求，是在经济社会发展进入新阶段和新的历史起点上，进一步推进信息化与经济社会发展的全面、深度融合的内在必然要求。

我国信息化发展战略的颁布和实施，是在经济社会发展进入新阶段和发展理念向科学发展观转变的过程中形成的。从信息通信技术发展的角度看，有两个非常重要的事实：第一，目前，我国拥有全球规模和容量最大的信息网络基础设施；第二，在全球互联网日益普及和互联网应用日益深化的条件下，我国已经成为日益重要的、新兴的互联网应用和服务市场。这两个基本事实构成了我国实施信息化发展战略的最基础条件，也是党中央、国务院部署实施信息化发展战略的基本前提。把信息通信技术的应用和发展作为一个战略议程，体现了我国经济社会发展的内在要求，也顺应经济全球化和信息技术变革的时代脉搏。

信息化发展战略背景要从两个方面来看：国际背景和国内背景。

1.《战略》出台的国际背景

国家信息化发展战略编制的国际背景是，信息通信技术革命与经济全球化这两个特别重要的观察问题的维度。我们知道，根据以往的经验规律，信息通信技术革命基本上每 10 年就跨越一个大的台阶。与以往三次大规模技术革命相比，信息通信技术革命除了带有以往技术革命的特点之外，其非常重要的特点是通用目的技术(General Purpose Technologies)。通用目的技术，自身具有应用面广、渗透性强以及发展和改进空间大等一系列特点，是三千多年人类技术变革史上所形成的蒸汽机、铁路等所无法比拟的，带来了无比广阔的生产率改进空间。同时，信息通信技术又是一种使能性的技术(Enabling Technology)，它可以带来不同技术之间的广泛互补性，可以与现有的人们已经熟练掌握的各种各样的技术类型密切融合，不仅促进了各类技术的相互适应、转换和创新，而且推动了各类产业的融合，不同产业之间边界越来越大，各类产业之间的界限越来越模糊。新技术、新产品，以及基于新技术、新产品所提供的新服务以及新产业迅速发展，且成为经济增长的新的来源。这就是技术与经济相融合的结果。

从全球化角度来看，信息化与全球化的相互交融和密切互动，使得全球的劳动分工不断深化，产业转移的速度不断加快；同时，各国和一些特定的区域经济结构调整步伐也不断加快，信息化已成为全球化形势下构筑国家竞争力的重要手段和力量之一。

信息通信技术变革最为特征的事实例证就是互联网的发展。互联网的渗透性、扩散性以及它所带来的应用效果，可以说已经席卷了全球各个角落，构成了经济社会活动的新空间。对于那些已经习惯利用互联网的人来讲，互联网就是信息通信技术的最神奇应用。互联网作为信息交流、传播和知识扩散的新载体，不仅有效地“消除”了人们沟通和交流中

的时间和空间的限制，出现了“无论何时何地”、“无论何人何种装置”等这样一些流行的关键词，产生了“地球村”，而且也带来了各种思想和文化之间的激烈碰撞。而从互联网本身所具有的网络外部性和正反馈过程——也就是说随着互联网人数的不断增加，其收益不断增加——来看，无论是电子政务、电子商务、远程教育、远程医疗，还是网络科学共同体（e-science）、电子社区，甚至包括信息网络基础设施自身的延伸和扩展，他们整体上构成的社会经济效果已经受到了与日俱增的关注，当今世界各国政府无不对此予以高度的关注。因为信息网络基础设施正在向无处不在的公共基础设施的方向演进，推行电子政务正在成为提高行政效率、扩大民主参与、建设效能型政府的重要手段，信息资源开发利用受益于信息传输范围、速度、手段和其受众面的不断扩大，不仅改进着人们的学习方式，而且可以改进人们对当期经济社会发展状况的评估和对所处发展阶段的识别[QH2007]。

进入21世纪以后，无论是发达国家还是越来越多的发展中国家，都纷纷把推进国家信息化看成是一个国家的重要发展战略，以期在新一轮的全球竞争中提升自己国家的综合国力。

2.《战略》出台的国内背景

制定和颁布实施国家信息化发展战略有其客观必然性。

(1) 从经济社会发展的背景来看，“十五”期间，中央在全面建设小康社会的过程中，不断总结改革开放以来的发展经验，沉着应对发展过程的问题，对发展理念、发展模式作出了重大的调整，高瞻远瞩地提出了科学发展观，强调统筹协调、以人为本，切实转变经济增长方式，建设资源节约型社会和环境友好型社会。随着“十五”时期我国经济增长和社会转型的速度加快，中央果断地提出了构建社会主义和谐社会的决策，并在最近做出了《关于构建社会主义和谐社会若干重大问题的决定》，应该说我国经济社会发展处在新的发展阶段和新的历史起点上。推进信息化，走新型工业化道路，正是目前推动经济结构战略性调整、转变经济增长方式，推进创新型国家建设、构建社会主义和谐社会的迫切需要。

(2) 从信息化建设自身的情况来看，加快推进信息化发展的基础条件已经具备。我国的信息网络基础设施实现了跨越式发展，成为日益重要的支撑经济社会发展的关键基础设施。无论是市场规模还是市场容量，我国的信息网络基础设施都已经占据世界第一位，互联网的应用成为国际社会一个新型的具有巨大应用潜力的市场，网民的数量已经占世界第二位，广播电视也基本覆盖了全国所有的行政村。从信息产业发展来看，信息产业规模在不断扩大，技术能力不断加强。“十五”时期是我国产业规模不断扩大、技术能力不断加强的很重要的时期。信息产业增加值在“十五”末时，已经占到GDP的7.2%，对经济增长的贡献每年达一个百分点，一批大型骨干企业的竞争能力不断增强[GJ2006]。

(3) 信息技术在国民经济和社会各领域的应用不断深化，效果不断显现出来。信息技术在第一、第二、第三产业的应用与以往的时期相比获得了长足的进展。农业信息技术的应用加快了传统农业改造步伐，农村信息服务体系在不断地拓宽、不断增强。按照农业部门统计，针对农业的信息服务网络已经覆盖了全国78%的地市，77%的县和47%的乡镇，涉农信息服务网站在全国已经超过了6000家[GJ2006]。

在传统产业的改造和升级方面，信息技术应用的效果也非常显著，特别是在装备制造业上体现的非常明显。在一些关键的工业部门，如电力、能源、化工、机械制造等，信息技



术得到广泛的应用，可以说这些部门脱离了信息技术的应用已经无法想象。信息技术的应用在传统工业的改造和技术升级方面取得了明显效果，普遍改进和提升了传统工业的劳动生产率。尽管在各类工业部门劳动生产率的测算中，因为统计数据的口径和方法上的原因，我们无法准确地测算信息技术对传统工业部门资本深化的效果，但是我们相信，"十五"时期国有控股企业劳动生产率的大幅提高和资本深化，一个非常重要的来源可能就是来自于信息技术的应用[GJ2006]。

在服务业方面，特别是在金融服务、现代物流等方面，可以看到，信息技术应用已经使得现代服务业发展成为带动经济结构战略性调整的先导部门，同时，基于互联网的各类新型服务业，不仅拉动了现代服务业的发展，而且成为传统服务业改造的引擎[GJ2006]。

在社会事业的各个领域，无论是在科技、教育，还是公共卫生、社会保障等领域，信息技术应用的效果呈现显著。比如农村中小学现代远程教育网络，仅就西部而言就已经覆盖了25％的西部中小学。在公共卫生方面，全国90％的县级以上医院和30％的乡村卫生院都实现了对法定传染病和突发性公共卫生事件的网络直报，有效控制了疫病的传播。在社会保障领域，各地基本上建设了社会保障综合信息系统，以人为本，方便老百姓获取社保方面的服务[GJ2006]。

(4) 电子政务建设稳步推进。围绕深化行政管理体制改革、政府职能转变、建立法治型政府、责任型政府、效能型政府和服务型政府的要求，政府管理的创新步伐不断加快。从上个世纪九十年代初开始建设的"金关"、"金税"和"金卡"工程，到"十五"时期陆续建设的其他重点信息系统，如"金盾"和其他一些综合性的系统，在改进宏观调控、实现有效市场监管、加强社会管理、改善公共服务等方面发挥了重要作用。各级政府的一些重要信息系统，边建设，边发挥作用，按照深化行政管理体制改革的要求，切实推进政府职能不断适应完善社会主义市场经济体制的需要[GJ2006]。

(5) 信息资源开发利用不断推进。随着社会主义市场经济地位的初步确立，市场经济体制的不断完善，经济社会活动对信息的获取、处理和传输的需要不断增加。目前，整个社会的信息资源意识已经显著增强，满足市场需求的信息资源开发活动和信息市场日益繁荣活跃，公益性信息资源开发利用获得长足进展，同时基于互联网的信息服务迅速增长。在"十五"末期，以中文为主的在线数据库服务网已经达到30.6万个，年均增长在60％左右。同时，基于互联网的中文网页数量快速增长，"十五"后两年复合增长速度大约在100％以上[GJ2006]。

此外，信息安全工作不断加强，特别是对基础信息网络、重要信息系统的安全防护，伴随着信息化应用日益深化，全社会信息安全意识也不断增强；我国信息化发展的环境不断改善，无论是法治环境、标准化工作，还是人才培养等都呈现出与时俱进的良好局面[GJ2006]。

在此基础上，《战略》提出了到2020年信息化发展的目标，即，综合信息基础设施基本普及，信息技术自主创新能力显著增强，信息产业结构全面优化，国民经济和社会信息化取得明显成效，新型工业化发展模式初步确立，国家信息化发展的制度环境和政策体系基本完善，国民信息技术应用能力显著提高，为迈向信息社会奠定坚实基础[GJ2006]。

《战略》提出了"一个转变、两个跨越、三个水平、四个能力"的目标。"一个转变"是指

“促进经济增长方式的根本转变”;“两个跨越”是指“实现信息技术自主创新、信息产业发展的跨越”;“三个水平”是指“提升网络普及水平、信息资源开发利用水平和信息安全保障水平”;“四个能力”是指“增强政府公共服务能力、社会主义先进文化传播能力、中国特色的军事变革能力和国民信息技术应用能力”[GJ2006]。

《战略》目标统筹兼顾信息化的重点领域和基础环境,妥善处理长远与当前的关系,同时,既考虑了国内经济社会发展的需要,也考虑了全面参与国际竞争的需要[GJ2006]。

《战略》所提出的十项目标,主要包含两个方面:一是通过信息技术应用,促进我国经济社会又快又好发展,主要体现在促进经济增长方式转变,提升政府公共服务能力、社会主义先进文化传播能力、中国特色的军事变革能力和国民信息技术应用能力等方面,体现了我国信息化和经济社会发展各个领域的要求;二是信息产业发展、信息技术创新、网络普及、信息资源开发利用和信息安全保障等方面,侧重于为前者提供基础和保障。由于信息技术发展变化快、渗透性强、涉及面广,《战略》没有明确提出未来十五年的数量指标,只提出了导向性的定性指标[GJ2006]。

在党的十八大上,胡锦涛同志所做的题为《坚定不移沿着中国特色社会主义道路前进为全面建成小康社会而奋斗》的报告中,更是有 19 处表述提及信息、信息化、信息网络、信息技术与信息安全。更重要的是,报告明确把“信息化水平大幅提升”纳入全面建成小康社会的目标之一,并提出了走中国特色新型工业化、信息化、城镇化、农业现代化道路,促进这“四化”同步发展。这充分反映了在我国进入全面建成小康社会的决定性阶段,党中央对信息化的高度重视和认识的进一步深化[GJ2006]。

此后召开的十八届三中全会所发布的《中共中央关于全面深化改革若干重大问题的决定》中则是着重强调了国家对信息安全的重视,强调要在新型城镇化建设中融入智慧城市的概念,在转变社会治理方式中加强数字城管和数字社管的建设,强调要加强金融、税务、政府、教育、医疗、司法领域的信息化建设为改革助力。此次会议的亮点之一是设立了国家安全委员会,确保国家安全,其中就着重提到确保国家网络和信息安全[GJ2006]。

信息发展战略是一个涉及方方面面的长远计划,它对我国 ICT 供应链的发展也有着深远的影响。实施供应链管理就要实施 POS 系统、EOS 系统、数据库系统的共享,EDI 和 VMI 在供应链管理中的应用,加速了 Internet 商务发展,而这些都和信息发展战略密切相关[GJ2006]。

信息系统将充分利用 EDI、XML 技术,建立统一数据交换平台;RFID 的出现和 GIS、GPS、GSM 技术的广泛应用,加强了信息的共享并加快了信息的流动,提高了信息的交互率;各种基于网络和 Web 服务的信息系统的建立、DCOM、RMI 及 CORBA 架构平台的应用,是实现各信息系统分布式应用的基础;人工智能(AI)、神经网络和系统动力学等智能技术,将为开发供应链的高度智能信息系统提供支持;数据仓库和数据挖掘技术的应用,对提倡个性化服务,有效衡量和挖掘客户价值有着不可估量的作用[GJ2006]。

10.24 我国 ICT 供应链发展所面临的风险

在第 9 章已经讨论过 ICT 供应链的安全问题,下面将着重讨论我国 ICT 供应链发展所面临的风险。

现在供应链安全风险问题,要从两个角度来看,一个是生产者,一个是消费者。生产者的角度,主要是说信息技术的产品是一个不断集成和加工制造的过程,每一个部件都有可能来自不同的地方,整个产品需要进行较多的采办和集成阶段,因此容易产生风险。从消费者来看,如何确定产品只执行它应有的功能而不存在后门,没有明显的缺陷和漏洞,这需要检测制度和相关机构。实际上,漏洞分析和风险评估的工作,就是对这种潜在的安全漏洞和隐患、风险进行相应的检测分析和评估。在国外,最终消费者,如一些大的行业用户,有权要求生产商出具产品供应链的安全证明。比如美国国防部有专门的国防产品供应商,并且要求供应商具备所提供产品各个部件的产地证明。有了相关证明,进而要求信息技术产品通过相关的安全评估,如基于国际通用领域安全评估准则CC的EAL等级评估,这就是一个较为可行的方法。

结合我国信息化发展情况和产业发展状况可以得出,目前我国信息产品供应链综合风险等级较高。一方面,从整个供应链的环境来看,设计、生产、制造信息产品,特别是中高端产品,有些未经安全性分析和检测就进入了应用环节,甚至是直接应用在某些重要部门,这是很危险的。另一方面,相关制度性的安排还不完善。我国是信息产品消费的大国,关于信息产品消费者权益保护方面,特别是软件产品缺陷召回制度和厂商责任认定缺乏相关法规。所以说我国面临的风险系数整体来说较高。

具体来说,我国ICT供应链安全突出风险反映在以下三个方面。

(1) 系统性风险,系统性风险是对国家信息安全制度可控性的威胁,也是对国家信息安全自主可控的挑战。反映在我国,就是缺乏完善的信息产品供应链安全管理制度安排。

(2) 产业型风险,反映在信息产品核心技术和知识产权还不属于国内产业;自主原创的技术比重小,价值低;国外资本通过收购和控股等方式控制国内技术和市场。具体来看,我国自主可控弱势局面短期难以改变,尤其是供应链高端(CPU,操作系统,基础应用软件等)技术还牢牢掌握在别国手中。关键技术的服务依赖于人,大量信息技术服务依靠国外,产品和系统的远程维护和外包服务普遍存在,网络基础资源受控于人,其中美国以绝对优势继续把持国际互联网根域名和IP地址的分配权、漏洞资源的掌控权乃至信息资源的绝对占有权以及相关信息传播的主导权。

(3) 用户性的风险,反映在某些高端信息产品如银行、电信、金融集团中使用外资品牌产品,以及某些信息服务由国外厂商提供,形成了专业术语称为供应商锁定风险,一旦被锁定就会不自觉地高度依赖,无法变更产品及服务供应厂商,因为变更供应商会带来原来投资保护及技术变化的不确定风险[FedEx2006]。

10.2.5 制约我国ICT供应链管理的因素

从整体上看,我国企业管理的总体水平仍然比较低,与发达国家相比还存在较大的差距。供应链管理在我国企业推广应用也面临着很多制约因素[L2004]、[LYQ2008]。

1. 社会环境还不完善

社会制度环境是企业供应链管理赖以存在的基础,目前来看,我国社会制度环境还没有为供应链管理提供足够有效的保障。我国企业实施物流和供应链管理发展所需的制度环境有待进一步改善,如融资制度、产权制度转让、人才使用制度、社会保障制度等,这些

制度是实现企业资源重组,创建新型供应链管理的前提条件。

供应链管理在我国尚处于发展初期,此时政府应大力发展和支持供应链管理的实施,包括资金、法律、政策上的支持。而实际上,现在政府在法律、政策方面给予的支持十分有限,政府对企业经营行为的规范和管理,有些方法也与供应链管理的要求不相适应。

市场是供应链运作的场所,供应链的有效运作需要在一个完善的市场经济环境下进行。我国目前正处于由计划经济向市场经济转轨的过程中,市场发育还不成熟,成为供应链管理的“瓶颈”。市场秩序不规范为供应链的建立增加了难度。供应链是具备不同核心能力的企业为追求联合效益而建立的,目的是希望通过合作实现更好的效益,因此供应链的建立需要一个良好的市场环境,要求企业之间按照市场经济规则进行资源和利润的分配。我国目前市场秩序不规范,强买强卖、以大欺小等不公平交易时常发生,严重影响了供应链企业之间的关系,增加了建立供应链的难度。

供应链上的企业同步化运作需要完善的市场体系来保障。不仅要有生产资料和消费资料等基础市场,还要有资金市场,劳务市场、技术市场、信息市场、房地产市场等生产要素市场以及各种配套服务市场等。我国目前市场体系还不完善,使供应链正常运作失去了植根的土壤。

中国的商业经营中,供应网络成员之间难以形成获取长远利益的竞合关系,战略经营联盟的形成存在较多的障碍,交易成本居高不下,极大地提高了供应链形成的“门槛”。传统商业文化和商业道德中的一些落后的东西排斥和拒绝供应链管理制度和文化,这些都在阻碍供应链的生存和发展。

供应链管理要获得长足的发展,人才是一个关键问题。首先,供应链管理理念在我国刚刚引入,国内企业界人士对此知之尚浅,更缺乏对供应链管理人才的教育和培训。其次,供应链管理是一种跨行业、跨部门的管理理念,它涉及诸多领域的高新技术,不仅需要专门的技术人才,而且需要及精通供应链管理理论、方法、手段,又熟谙与供应链相关的诸多技术的综合性人才,以保证在供应链某环节发生故障时,他们能统观全局,给予合理的解决。

虽然市场对物流与供应链管理人才的要求不断提高,但目前我国物流与供应链管理人才教育和培训方面还存在较大差距,无论是学历教育还是非学历教育,都不能很好地满足对物流与供应链管理人才的需求。

虽然现在不少院校开设了物流管理和供应链管理专业,但由于供应链管理是一门综合实践性学科,是技术与经济相结合的边缘学科,供应链管理中需要使用大量的先进技术和手段,一般管理人员往往无法掌握这些技术与手段的精髓,在现阶段的供应链管理实践中,往往可以看到供应链管理有明显的纯技术性趋向或者是纯管理性取向。所以发展供应链管理,不仅需要高级管理人才,更需要大量执行型与操作型人才。

我国现阶段供应链管理人才缺口原因表现在以下两个方面。

(1) 我国对供应链管理的研究还处于引入阶段,具备扎实理论功底的人才稀缺,更不用说实践与理论兼备的高级人才。

(2) 缺乏既具有管理技能,又具有基本操作功底的综合性人才。供应链管理是一种综合性的管理措施,它要求管理者既熟悉物流环节(包括采购、运输、仓储)、信息环节



（包括信息系统的设计、运行、监控等），又具有协调、组织、指挥等相关的基础管理能力；要求管理者不仅具有大局观、系统观，更应该具有“见微知著”的能力。而我国企业大部分是从计划经济的计划控制模式逐步转向市场经济模式，在计划经济模式下培养出来的管理干部，仍然存在着“偏而不全”的问题。虽然近年来在西方管理理论的影响下，我国企业效仿西方企业使用了职位轮换等方式充分锻炼管理人员的综合管理技能，但这些管理人员也仅仅是“杯水车薪”，不能充分解决现存的问题。

2. 供应链设计、管理基础薄弱

管理是企业发展的永恒主题。随着时代进步和经济发展水平的提高，企业管理必须不断创新。在供应链管理的初步实施过程中，我国企业在管理方面不适应供应链管理的弊端日益暴露，主要表现在两个方面：企业管理观念落后和管理机制不健全。

信任是供应链中各企业进行有效合作的纽带与保证，供应链企业之间的相互信任是供应链发展所必需的。而就目前来说，诚信问题给企业和整个社会经济的发展造成了很大的障碍，显然不适应供应链管理的需要。我国许多企业眼光过于狭隘，过多地看重眼前的经济利益而忽视长远利益：一方面，很多企业管理者存在短视行为，看不到实施供应链管理将带给企业的更多更长远的利益，而主观地认为业务外包是对企业自身生产经营权利的一种侵犯，认为即使是非核心的业务，如果交由别的企业去经营，也是“肥水流入外人田”，不愿意与其他企业结成战略合作关系。另一方面，许多企业为了追求经济利益而忽视了自身的信誉与商业道德。许多企业都从自己的利益出发，尽量地将责任、风险、成本等转嫁给其他与其有商业往来的企业，却竭尽全力地将利益收归己有，使供应链运作很难达到预期效果。

一个发展前景良好的企业，才是供应链战略伙伴的最佳选择，才能为供应链发展做出应有的贡献，才能有效地提高供应链管理的绩效。但是目前，我国绝大部分企业都无法有效的实施供应链管理，企业管理基础薄弱是原因之一。而造成企业管理基础薄弱的成因则是多方面的，包括企业战略选择不清晰、企业战略与供应链战略不相符等等。

企业战略是指导企业运作的原则性纲领，在企业运营过程中占有主导性地位。它不只是一个口号，也是企业运营过程所应该遵循的章程，它应该清晰明确的表达企业的运作目标，而且一定要在企业的运营过程中身体力行。然而，我国绝大多数企业所建立的企业战略往往都是一句空头口号，往往表达不清楚，没有深入贯彻执行，有些企业甚至没有制定相关的企业战略，从而导致了企业的运营过程毫无依据。供应链战略联盟是企业的组合体，它和单个成员企业一样也需要供应链战略来指导其运行，因此，成员企业的企业战略就成为供应链管理战略的支撑，如果成员企业没有明确的企业战略，那么整个供应链战略必然会出现问题。从我国供应链管理实施的现状来看，在制定、实施供应链管理战略这方面做得不是很好。在考虑诸如本供应链战略联盟为什么会存在、该供应链战略联盟能带来什么样的运作结果、该供应链战略联盟成员企业之间的连接关系等等问题时，成员企业尤其是盟主企业往往没有一个比较明确的答案。于是，供应链战略就名存实亡，根本没有起到协调、激励、监督供应链战略联盟成员企业的作用，因此造成供应链管理绩效低下也就不足为奇了。

我国企业缺乏有效的激励机制。我国企业管理的激励机制主要侧重如何调动企业内

部员工的积极性来实现企业自身效益的最大化，而很少涉及激励供应链中的企业对其核心竞争能力进行培育与创新。

营销渠道管理中，最困难的问题和障碍在于如何使制造商与渠道成员、特别是零售商之间通过信息资源共享来消除需求管理中的不确定因素。幼小的零售商更多考虑的是尽可能建立和保持有利的谈判优势，不情愿让制造商利用自己获取的详细的客户购买情况的信息资料。制造商为了实现消除需求波动因素、提高运转效率的目标，不得不在通讯、信息、物流、分销、结算、融资等众多业务中大量投资，这实际上增加了制造商经营的不确定性和风险。海尔公司在推行业务流程再造的过程中，与上游供应商的业务整合成效显著。尽管多年来营造了最大程度控制的营销渠道，在国内公司中最有条件与零售终端合作进行客户关系管理，但这项工作目前只能实现对零售终端的需求迅速反应，至关重要的消费者需求预测和管理还难以充分实现。

3. 企业组织结构不适应供应链管理

我国企业整体组织结构设置普遍落后，还未能达到完善的物流管理所要求的对企业内部功能、流程的一体化阶段，离供应链管理所需的外部一体化要求就更远了。这是因为企业对现代竞争理论的认识还不够，仍停留在传统竞争理论阶段，未能充分认识到竞争已向供应链竞争转型，对物流管理的认识非常模糊。

传统企业组织是按职能分派责任的，如采购职能、产品职能、销售职能等。实行高级主管领导“垂直”职能，不容其他职能侵入。这种垂直职能还反映在预算系统中。每个职能都由预算驱动，以控制职能消耗，公司好似运行于消耗之上，它们最基本的目标是控制、增加利润输出，把输出作为组织、计划、控制的基础。就是说，它是以增加整个系统库存为代价的。这不仅增加了财务负担和流动资金，还降低了最终需求的可见度。从而使上游活动对下游的真正需求无任何清晰的观点。传统组织的另一问题是费用“透明度”低，因为传统组织处于高度的聚积状态，一般只在其职能基础上辨别费用。在传统企业内部，每个人都习惯于关注系统中单一组件的效率，而没有人去考虑整体效益。例如，运输部门追求低运输费用，采购部门愿意增加订购量以减少单价，销售部门希望高库存以减少缺货损失。在传统企业之间则更无信息共享、通力协作之说。所有这些部门都同供应链管理相冲突。

10.3　我国 ICT 供应链安全问题的应对

目前我国一些具有前瞻性战略眼光的企业已瞄准了供应链管理这一管理方法并加以运用，它对于我国企业因规模小而不能形成规模效益，因其结构全、开支大、内部层次繁多、结构臃肿而不能形成合力，大多数企业重复低层次竞争而导致两败俱伤等问题都提出了一种全新的解决方法。但在具体实施过程中，因为我国独特的国内经济环境及长期形成的企业内部管理特色及别具一格的企业文化，导致了一些不同于西方的问题的存在。

10.3.1　中美 ICT 供应链安全问题对比

(1) 中国面临比美国更为严重的供应链安全威胁。这一境况不言而喻。目前，来自



国外的ICT产品和服务在我国市场上占绝对的垄断地位，国家的很多基础信息网络和重要信息系统甚至采购了清一色的国外ICT产品和服务。这相当于洞开国家安全的大门，使我们比美国更有理由担心ICT供应链安全问题。因为，美国的担心主要是理论上的，而我们的担心则完全是现实中的。

(2) 中国的ICT供应链安全问题受到技术方面的巨大制约。我国ICT供应链安全问题的核心，是自主可控能力不强，产品和服务严重依赖国外，我们往往不得不面对"巧妇难为无米之炊"的局面，这使我国在解决ICT供应链安全问题时受到巨大的技术制约。我国的ICT供应链安全管理对策不得不考虑到这一具体情况。

(3) 中国的ICT供应链安全问题受到WTO规则的巨大制约。美国拥有的巨大的技术优势使其在解决ICT供应链安全问题时从容不迫，方法多样，且美国在很多制度设计时已经充分利用其在WTO的话语权巧妙规避了WTO规则。例如，在我国联想集团并购IBM个人电脑业务时，出于对供应链安全的担心，美国政府曾试图否决此项交易，在美国政府最终与联想集团签订的协议中，美国也施加了大量的限制性条款，例如禁止联想为政府部门提供计算机售后服务。这是对贸易的明显限制，但遗憾的是，并购业务并不属于WTO规则管辖的范围。而我国由于缺少技术优势，可用的手段比较单一，暂时可能需要借助政策手段，但这很容易触及WTO规则的限制[Z2010]、[BPG2012]、[J2009]。

10.3.2 我国ICT供应链信息管理存在的问题

我国供应链信息管理尚处在起步阶段，供应链信息管理在我国具有巨大的挖掘潜力和长期的发展前景。但是就目前而言，我国供应链信息管理面临着制约其发展的瓶颈[H2010]。

(1) 企业的信息化水平高低不一。企业供应链信息化程度不等加大了实施供应链信息管理的难度。一方面，很多企业，如联想、长虹、海尔等，通过安装ERP系统或其他管理信息系统提高管理信息化程度，企业各部门能利用实时的生产、库存、销售和财务数据及时做出正确的经营决策。另一方面，由于管理信息系统的购买、安装和维护费用较高，一些企业出于成本和人员方面的考虑，信息化起步较晚。

(2) 中小型企业的信息化程度低。中小型企业的信息化程度低是制约供应链信息管理发展的首要瓶颈。据2003年的调查数据显示，我国北京地区的企业中采用信息系统进行管理的尚不足30%，远远低于发达国家的水平，这极大地阻碍了我国物流信息化的进程，而造成这一现状的主要原因是各个中小型企业的起点都很低，而大多数的信息管理系统的成本较高，市场上缺少真正适合中小型企业的信息系统。由于信息化水平低，企业搜集、处理和利用信息的能力较差，就更谈不上与其他企业进行信息共享与合作了。此外，即使有最先进的软硬件，如果不能在决策中充分利用采集到的信息，那么信息化仍然停留在较低的层次上。所以企业应该着眼于信息利用，而不仅仅是信息的采集[H2006]。

(3) 缺乏拥有自主知识产权的供应链管理信息系统。缺乏拥有自主知识产权的供应链管理信息系统是我国供应链信息管理的瓶颈之一。以我国目前的国内软件研发能力及研发水平来看，尚无法和国际上的同行们竞争。而且供应链信息系统在标准上还未形成体系，较为混乱，各个企业间的供应链信息系统都是各自为战，难以互联互通，实现信息

共享。

(4) 软件开发商难以盈利。供应链信息系统软件也是管理软件,各个企业对软件的需求不同,要求的标准也不同。因此软件需求的个性化和生产的批量化难以得到统一。对于软件的开发商来讲,个性化的需求导致研制开发软件的成本极高,不能进行批量生产。另外,由于缺乏对于信息技术的规范和开发模式的规范,加之企业对个性化需求的进一步增强,这些都使软件开发商们陷入了进退两难的境地。

(5) 基础信息和公共服务平台的发展滞后。良好的信息管理软件需要完善的基础信息和公共服务平台的支持。而就我国目前情况来看,基础信息和公共服务平台的应用比例很低,根本无法保障信息管理软件的正常应用。如全球卫星定位系统(GPS)和地理信息系统(GIS)技术服务在我国大型企业的应用比例很小,而在中小型物流企业,此类技术服务基本上是空白。这种基础技术服务的应用比例过低,直接导致了物流信息化的低效和整个行业的整合困难。

(6) 数据标准不统一。目前在我国,企业供应链的数据标准尚未统一。以消费品为例,很多商品(超市的生鲜食品)都没有条码,零售企业为了方便前台销售和实现内部管理信息化,必须通过配送中心给商品贴上内部编码。这样做既增加了商品本身的成本,又不利于信息系统之间的数据传递。另外,由于各个企业采用不同的格式编制和保存数据编制商品代码,也给供应链信息化设置了障碍。为了使数据标准统一化,企业不得不投入资金开发或购买新的软件,对企业供应链的信息进行编译,使各方都能读懂和利用这种信息,这样无疑增加了信息管理成本。

(7) 信息传递不顺畅。由于供应链中的不同企业安装的硬件产品和信息系统不同,导致数据接口不一致,也是信息传递不畅的原因之一。另外一个企业往往同时处于很多条供应链中,可能要面对很多企业,使得在企业供应链与企业之间直接传输数据的工作量非常大,管理起来比较困难。

(8) 信息共享程度小。供应链信息管理要求企业与企业之间及时地交换和更新信息。有观点认为供应链信息管理作为企业信息化的一个主要方面,要求链上的各个节点企业实现高度的信息共享,技术的、资源的、运行策略的、生产的、库存的各类数据集成是供应链运做的基本保证,共享程度的高低决定了供应链的效率。但在实际运作中,供应链中每个企业是有自身利益的实体,它们的目标不可能完全一致,甚至会有冲突,因此不可能也没有必要将全部信息与别的企业共享,而要共享的部分则是能够为各方带来效益的信息,如库存数据、需求预测、促销计划等。此外,信息共享程度的高低除了取决于信息的类型之外,还取决于企业利用供应链中信息的能力。如果一个企业不能正确使用别的供应链其他成员提供的信息,那么占有大量信息不但不能产生效益,反而可能误导企业的经营决策。

10.3.3 我国 ICT 供应链安全问题对策

供应链必须要有法律原则来做保证。首先供应链从原料环节起必须是清晰的;其次就是产品系统和服务,必须有自己的底线。底线的根据其实就是法律,法律变成标准,标准才能变成实际应用,比如处理过程、集成过程、建造过程等等,都得落实实处。此外就是



持续的监督和检测[L2004]、GMZ2003]。

解决供应链安全问题是一场持久战，要形成一种习惯，绝对不能做运动方式的一阵风。同时，在解决问题的过程中，一定不能忽视技术上的自主和创新。为应对这些问题，我国提出了以下策略。

(1) 加快供应链安全制度建设，落实自主安全可控战略。具体来说，就是研发方面，要推动自主研发和知识产权保护，从国内来看，提升产业的自主创新能力是根本，这就要求我们成为技术、产品的供应者，成为自己能生产、制造和创新的大国。这个目标是需要国家的大力及长期政策、资金、技术支持等才能达到的。

流通方面要建立产品原产地证明。希望我国今后能在软件代码、硬件的芯片上实现像传统意义上的产地身份证明，即软件代码属于哪一家公司开发的，要有能够查验的电子化的身份证书，具备唯一可靠的标识，这就从某种程度上加强了对生产者的管理，这是最终要走到的一步。在全球化的情况下，供应链的风险是一直存在的，因为现在外包和开发，以及生产一个产品，经常具有多样的生产地及复杂的技术、货物流通环节。因此解决这个问题，就和网络空间里要解决个人上网实名制的问题一样，未来网络设备、软硬件设备的身份问题也需要解决，这样产品一旦出问题即可追溯。整个供应链安全，要求不仅仅是最终产品的生产厂家责任实名、可追溯，还要求各个环节的责任可追溯，各环节中责任划分还需明确。采购方面要构建非关税的技术壁垒，并且要求进行安全性的分析、监测。除了海关部门的检查，还需要有相应质量监督部门进行把关。使用方面引导用户重视供应链风险。关于消费者、最终用户、行业的用户，在采购信息技术产品的时候，可以要求对所购买产品进行安全性检测。

(2) 国家应开展供应链安全漏洞分析和风险评估。在技术方面，应安全审查源代码、分析软件同源性以及建立硬件产品溯源机制。在产品方面，应主动检测和分析漏洞产品，开展自主原创证明。此外，国家还应开展服务管理，建立审查制度，对参与人员发放许可证，并推动产业链的整合，加强可控风险评估。

(3) 建议建立国家信息技术产品政府采购安全审查机制。我国正在进行加入《政府采购协议》的谈判，按照该协议的规定，政府采购要遵循国民待遇原则和不歧视原则，不得对国内供应商提供保护以及在国内外供应商之间实行差别待遇。针对我国大量采用国外信息产品的现状，建议参照国际通行做法，对境外产品采取风险可控策略。有关部门可考虑建立我国信息技术产品政府采购审查和评估机制。

同时，为遵循 WTO 原则，确保正常的贸易往来和需求，建议有关部门建立境外信息技术产品快速通关程序，有效化解政府部门面临的来自境外供应链信息安全风险，分担国家信息安全责任，这样有利于创建国内信息技术产品的良好生存和发展环境。建议将信息安全评测结果作为我国政府采购评价指标，此举既适应 WTO 体制下的国际经贸准则，又可将敏感的政治和安全问题转化为技术和非关税壁垒手段处理的问题，是维护国家信息安全、促进国家信息化健康发展的有效举措，也是欧美发达国家普遍采用的保护国内市场的做法。

(4) 在企业经营中引进现代管理思想。为了实现供应链管理，必须提高参与企业的信息水平，改变参差不齐的局面。信息系统的建设首先是一个管理思想的建设，要管理改

革在先,技术实施在后。实施信息管理是为了提高企业的效率,而提高企业的效率的关键一点就是要强化管理。要应用先进的管理理念与模式和现代信息技术对企业的管理进行根本的改革。因此,在信息化建设过程中,管理思想、管理体制的建设要自上而下,信息化的建设要自下而上。只有采取上下结合的方式,企业供应链信息管理建设才能取得成功。只有在优化经营过程、强化管理的基础上进行信息化建设,才能充分发挥信息化综合经济效益,也为实施供应链信息管理创造良好的先决条件。

在管理的具体实施上一是要加强对ICT供应链安全的战略研究,对我国的ICT供应链安全管理政策提供充分的战略研究支持;二是要加大宣传力度,提高广大用户特别是基础网络和重要信息系统的主管和运营单位的信息安全意识,提高政治觉悟。对于国产产品可以满足使用需求的,要引导其自觉使用国产产品;三是要抓紧提高对国外产品和服务的替代能力,鼓励国产产品试点,建设国产产品试用平台;四是要认真做好信息安全产品认证工作和漏洞检测分析工作,加强技术防范;五是要逐步由粗放型管理向精细化管理迈进,要探索在对产品采购、使用管理的基础上开展对产品生产、流通的管理和对人的管理;六是标准化,为了提高供应链的灵活性和风险发生后的快速恢复能力,标准化十分重要。在产品设计中引入标准化,使用通用的部件或替代性很高的部件,不但能提高生产的灵活性,而且能保证零部件的供应。即使原有的供应商不能准时交货,公司也可以迅速找到可替代的新供应商,从而更好地应对供应链风险。

供应链是一个复杂系统。链上任何一个环节出现问题都会波及整条供应链的每个环节。企业必须与供应链上下游共同制定风险防范计划,相互督促,进行供应链风险的识别、评估与管理,以达到整条供应链平稳、有效地连续运行,实现利益共享,风险共担。调研发现,我国企业对于风险管理特别是依赖于供应链成员间协作的供应链风险管理还缺乏深刻的认识。虽然有部分管理人员开始意识到风险管理的重要性,但是缺乏实际有效的行动。所以,我国企业应转变观念,充分重视供应链风险管理,与上下游企业合作,共同制定风险防范计划。

(5) 重构业务流程与系统。提高对顾客的反应能力。大规模定制是优化供应链,增强对顾客反应能力的一种有效的业务方式,是供应链管理挑战传统品牌经营战略的有力手段。大规模定制根据顾客的实际选择,进行一对一的直接联系,按订单制造和交货,在减少库存提高生产率的同时,充分了解和满足顾客的真正需求。通过业务流程与系统重组,简化业务流程,提高对顾客的反应能力,提供个性化产品和服务,增进企业与顾客之间及与供应商之间的长期良好的合作关系,降低企业的成本,提升企业核心竞争力。

(6) 提高条码的利用率。供应链管理需要参与企业充分交换信息,商品在供应链中流动时如果有一个统一的编码将极大地方便参与企业的信息管理和交流。比较理想的方案是制造商在其产品上按照国家标准打上条码,这样分销商、批发商和零售商都能使用该条码,能减少编码工作量,减小资金和人力的耗费,并有利于供应链各方交换商品的生产、库存和销代情况。

此外,企业供应链的数据和文件格式要尽量统一。例如主导型企业可以利用它在供应链中的影响力要求跟随型企业使用规定的格式压缩和保存数据及文件,而均势型企业可以通过共同协商确定数据和文件格式。



(7) 增强企业协作关系。在强化企业协作关系方面，我们可以从两个方面入手。一是统一供应链数据接口。在设计供应链管理信息系统时，应该预留专门的数据接口，便于企业从供应链上下游的合作伙伴处接收和发送数据，实现系统对接。文件传递方式或协议和使用的端口可以由供应链参与方共同确定。二是确定企业之间的数据共享程度。供应链参与方可以根据需要确定合适的信息共享程度。例如哪些信息应该共享，以及这些信息由哪些企业或部门共享。通常供应链管理要求物流信息、销售信息和供应信息在相关企业之间共享，以便及时对市场情况做出反应。

10.3.4　从国际安全的角度来看 ICT 领域的发展

近年来，最新信息和电信技术的开发和应用方面取得了很大进展，但这些技术有可能被用于与维护国际稳定与安全的宗旨相悖的目的。极为重要的是，必须通过国际合作和本着相互尊重的精神应对信息安全领域的共同挑战。为此，2011 年 9 月 12 日，中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦常驻联合国代表联名致函联合国秘书长潘基文，请其将由上述国家共同起草的“信息安全国际行为准则”作为第 66 届联大正式文件散发，并呼吁各国在联合国框架内就此展开进一步讨论，以尽早就规范各国在信息和网络空间行为的国际准则和规则达成共识。

这份“信息安全国际行为准则”文件就维护信息和网络安全提出一系列基本原则，涵盖政治、军事、经济、社会、文化、技术等各方面，包括各国不应利用包括网络在内的信息通信技术实施敌对行为、侵略行径和制造对国际和平与安全的威胁；强调各国有责任和权利保护本国信息和网络空间及关键信息和网络基础设施免受威胁、干扰和攻击破坏；建立多边、透明和民主的互联网国际管理机制；充分尊重在遵守各国法律前提下信息和网络空间的权利和自由；帮助发展中国家发展信息和网络技术；合作打击网络犯罪等。

近年来，信息和网络安全问题受到国际社会普遍关注，制订相关国际规则、规范信息和网络空间行为的国际呼声日益高涨。据了解，中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦提交的“信息安全国际行为准则”文件是目前国际上就信息和网络安全国际规则提出的首份较全面、系统的文件。

10.3.5　我国相应标准的发展及应对

国务院颁布的《鼓励软件产业和集成电路产业发展的若干政策》，从投融资、税收、技术、出口、分配、人才、采购等方面，为中国软件和集成电路产业发展创造了良好的政策环境。出台了《软件企业认定管理办法》和《集成电路设计和产品认定管理办法》；颁布了《中华人民共和国电信条例》、《无线电管理条例》、《互联网信息服务管理办法》、《关于维护互联网安全的决定》等有关规定，其他一系列规范电信市场竞争、维护电信消费者权益的法律法规正在制定之中，初步形成了开放的、公平有序的法制环境。这些规定的颁布也为 ICT 相关标准的公布奠定了基础。

目前，《供应链安全管理标准》《供应链安全管理体系——ISO/PAS 28000 实施指南》《供应链安全管理体系——实现供应链安全的最佳实践指南——评估和计划》《供应链安全管理体系——对供应链安全管理体系审核认证机构的要求》等 4 项国家标准正在制定

当中。这4项国家标准由全国公共安全基础标准化技术委员会(SAC/TC351)归口管理。全国认证认可标准化技术委员会(SAC/TC261)与全国公共安全基础标准化技术委员会(SAC/TC351)已建立合作机制。经双方研究决定,由SAC/TC261组织开展《供应链安全管理体系-对供应链安全管理体系审核认证机构的要求》国家标准的起草工作。同时,SAC/TC261选派认证领域专家参加《供应链安全全管理标准》《供应链安全管理体系——ISO/PAS 28000实施指南》《供应链安全管理体系-实现供应链安全的最佳实践指南——评估和计划》标准起草组工作。这些标准的制定,将为我国的供应链安全管理体系,提供一套较为完整的标准。

我国虽然一直很重视公共标准的制定工作,但是没有充分考虑标准的贸易和技术创新效应,在制定国家标准和行业标准存在一些不容忽视的问题。其中比较突出的问题有两个:

一是在国家标准和行业标准的制定过程中片面追求“高”标准,或片面强调与“国际标准”接轨,不利于公共标准促进贸易效应的发挥。从公共标准的贸易效应角度看,国家标准和行业标准等公共标准的功能是减少交易双方信息不对称,降低缺乏规范产生的交易成本,提高交易效率。因此,制定相关标准的目的是为了使交易的产品质量和等级等相关信息能够有效显示出来。质量和等级不同,交易双方会以不同的价格成交。这一类标准实际上是产品能够进入市场交易的“最低标准”,只要这个标准满足基本的安全、健康和环保要求。标准要求越高,能够进入市场交易的产品就越少,贸易的规模当然就越小。

由于我国与发达国家产业发展的技术水平不同,发达国家的某些“基本标准”对于我国可能就是“高标准”。在制定公共标准时如果不假思索地采用这些国际标准,其结果可能是有利于国内少数先进企业的对外贸易,却不利于我国大多企业的国内贸易。

二是在公共标准的制定中片面强调技术的先进性。从竞争和技术创新角度看,公共标准实际上是企业竞争和创新的一个基础,是企业进入市场的起点。公共标准所包含或反映的技术水平应该考虑一国大多企业的技术能力,或者一国平均的技术能力,而不应该追求技术的“领先水平”。因此,从公共标准的技术创新效应看,标准体现的技术成分和含量应该是比较稳定、成熟的技术。这不仅可以利用公共标准使成熟技术的相关信息充分的“显示”出来,而且还使公共标准很容易绕开私人专利,从而使相关技术能够更多的企业使用和共享,使公共标准的“外部收益”。至于相关标准制定部门所希望技术创新导向作用,应该由相关的知识产权保护机制去实施可能效果更好。

总之,在人们都关注ICT产业私有标准,关注ICT产业标准的知识产权问题及其影响的背景下,重新认识这一领域的公共标准的特点和经济功能,以及公共标准制定中存在的问题,对于充分和全面地考虑我国的标准化战略问题有着不容忽视的意义。从国家利益的战略高度看,在标准竞争中处于有利位置,至少从如下三个方面会获得明显利益[MFF2005]。

(1) 获得经济利益。信息产业中的利润分配遵循有名的“微笑曲线”,即在整个产业链中,处于两端的研发和销售的利润很高,而处于中间阶段的加工制造利润很低。中国的信息技术市场空间巨大。但是国内在技术和研发上投入少,创新能力不强。企业没有关键专利和核心技术,技术严重依赖国外,在产业链上处于下游和被动地位,在产品市场上



处于低端和被压榨的状态，利润率低。谁在竞争中掌控标准，谁就可以在整个产业链的利润分配中掌握主动权。在产业链中向上游发展，通过研发获得标准控制权，是中国企业摆脱“人为刀俎，我为鱼肉”局面，获得经济利益的必然选择。

(2) 提高科技能力和军事能力乃至综合国力。一个国家科技能力的提高根本无法仅仅通过技术引进完成，这一点已经为韩、日等国家的兴起和我国 20 多年的引资经验证明。这不仅是出于政治、军事原因无法获得国外最先进的技术，也因为先进技术的外溢和吸收不是一个结果，而是一个过程，需要本国企业有比较接近的技术能力。标准竞争必然要求先进技术的先导作用，这有助于提高一国的科技水平，从而提高国家的整体竞争力。

(3) 提高我们在其他领域讨价还价的能力。标准竞争举动本身，就可以在突破技术封锁和市场封锁方面发挥作用。比如中国的 3G 标准 TD-SCDMA 推出后，为打破欧美 3G 标准的垄断，为国内相关产业提供了发展空间。此外，是否采用标准，如何采用标准也会成为国际谈判中有利的筹码，为其他领域获得利益。

在全球化、信息化环境和“中国和平崛起”的背景下讨论标准竞争问题对中国国家利益的影响，其意义不可低估。从历史上看，自工业革命以来，先后崛起的国家都是以民族、国家为主体的。虽然激进的“国家过时论者”认为，在全球化的时代，民族、国家即将寿终正寝。但根据现实主义的观点，国家的某些作用在全球化时代更加突出。国际社会无政府状态对民族、国家，特别是像中国这样一个发展中大国来说，对国家主体性的要求更高。但是应该承认，全球化正改变着国家和国家体系间的关系。无论是军事影响力的下降还是国内与国际间互动的增强，都对一个国家在国际关系中的经济影响力提出了很高的要求。这种发展要求和消长关系的要求，正是政府干预产业标准制订的主要原因。

战略性贸易理论认为，如果考虑了规模经济不完全竞争和技术外溢等因素，政府的某些政策会有利于本国厂商取得国际市场中的支配地位从而为本国的“国家福利”带来好处。虽然许多经济学家，如格罗斯曼和克鲁格曼对采取战略性贸易政策的可能性和可行性提出了质疑，但根据战略性贸易理论的分析，我们有理由认为，对与标准问题密切相关的信息通信技术产业应该采取支持政策。

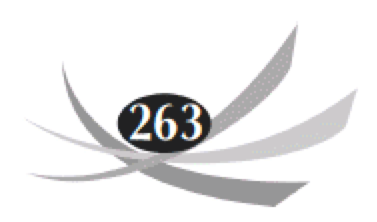
标准的制定应遵循以下原则。

(1) 采取先占策略争取在早期就取得市场领先地位。先占策略的理论逻辑是明显的，因为在存在网络效应的市场上，先行者具有先行优势，网络市场上正反馈效应的作用有利于先行者，而不利于后来者。先行者一般来说在网络规模上有先天优势，消费者加入先行者的网络可以比加入后来者的网络获得更大的网络外部收益，因此消费者对先行者产生一定的偏好，市场也随之会偏向先行者，而网络效应的作用会加速这种偏向作用，最终先行者的技术会成为事实上的市场标准。如在 PC 操作系统行业，微软占尽先机，在 DOS 操作系统成功之后，又不断地成功推出 Windows 操作系统。微软在 PC 操作系统上成为事实上的技术标准与它在市场上的占先优势有着重要的关系。前面所说的 QWERTY 键盘成为行业标准也主要是先占优势发挥了关键作用。当然，单靠先占策略也并非一定能获得成功，要取得成功还得靠其他战略的配合。如前面提到的高清晰度电视技术的案例，虽然日本在这一领域拥有先发优势，但在美国政府的努力下，最终却是美国自己研制的 ATSC 制式取得了成功[XMH2007]。

(2) 建立起基于企业联盟的政府引导的技术标准形成机制。技术标准的形成机制是产业标准战略的核心问题。技术标准的形成机制主要有市场机制、组织机制和政府主导机制。研究表明,对于 ICT 等高技术产业,在市场竞争比较充分的情况下,市场机制和政府主导机制都各有利弊。而通过组织机制形成自愿联盟标准,却是当代信息通信产业比较普遍的组织形式。从我国的情况看,目前很多企业的技术创新能力,特别是能够影响产业技术标准的创新能力还很薄弱,如果像美国那样主要采用市场驱动方式,虽然在技术选择上有可能产生最优标准,但其结果却很可能是跨国公司已经获得知识产权保护的事实标准进一步控制中国的高技术产业。鉴此,我国技术标准的形成机制可以考虑采用一种将政府主导机制和组织机制的优势结合起来的混合机制。企业联盟作为组织机制的一种形式,具有影响用户预期,支持相关企业进行互补产品开发,降低技术交易成本等优点。而且,依靠标准扩散的联盟推动力,更有利于率先建立起规模化的用户安装基础,从而在技术标准的市场竞争中赢得领先优势。所以,建立起基于企业联盟的政府引导的技术标准形成机制,是中国比较现实的选择。

(3) 充分发挥政府在技术标准化过程中的影响和作用。对于中国这样一个具有巨大市场优势,同时又处于技术赶超阶段的国家而言,政府在技术标准化过程中的作用,除了通过产业技术政策支持与技术标准开发相关的 R&D 计划,以及制定竞争政策规制跨国公司滥用知识产权的行为之外,还应该有更多的发挥空间。比如,政府可以有选择地对一些以国内企业为主的产业联盟给予资金和税收等方面的支持。特别是对 ICT 产业的众多技术而言,其技术创新过程主要集中在系统和产品系列方面单个企业独自开发面临较大的难度,而通过政府牵头的一些涉及产学研或企业间合作的 R&D 计划,以及政府对这类企业在资金和税收方面的支持,就更有可能在技术生命周期的早期阶段促进关键产品要素的标准化。目前,在数字电视产业的技术标准竞争中,中国数字电视产业联盟等组织就得到政府的大力支持。此外,在市场需求摇摆不定的情况下,政府的需求有时候也会成为决定标准存亡的关键因素。因为这时对于各种技术标准来说,谁能够最先获得大量的用户进而达到临界容量,谁就最有可能成为产业的事实标准。此时,如果能够适时地充分发挥政府购买力的影响,就会较大程度地提升中国技术标准的市场竞争力。

(4) 适当提高技术标准的开放程度。开放性既是技术标准的本质属性要求,也是决定技术标准竞争优势的基本因素。一般来说,通过市场竞争脱颖而出的技术标准都具有很高的开放度。例如,在 2G 移动通信技术标准中 GSM 的开放程度就明显高于 DAMPS,PDC 和 CDMA 等标准,共有 13 个运营商和 10 个以上的制造商参与了这项标准的制定。GSM 的广泛开放性决定了其具有很强的技术包容性,从而相比其他标准更容易得到推广使用。在技术标准专利化条件下,提高技术标准开放度的主要途径就是组建尽可能广泛的基于专利交叉许可的专利联盟。尽管目前中国正在制定的一些技术标准也相当重视扩大专利联盟的组成范围,比如到 2003 年,中国的 TD-SCDMA 标准的专利分布是:诺基亚占 32%,爱立信占 23%,西门子占 11%,大唐电信占 7.3%,高通占 2%,其他为 24.7%,但是与发达国家的技术标准,如欧洲主导的 WCDMA 和北美的 CDMA2000 标准相比,中国技术标准在开放程度上和联盟影响力方面的差距还很明显。因此,要进一步利用中国的市场优势,大力吸引以跨国公司为主的外国企业加入由中国



企业主导的专利联盟，不断提高中国技术标准的开放程度，以此提升中国技术标准在国际市场上的竞争能力。

(5) 尽快加强反垄断立法。在ICT产业我们面临一个问题，就是大的跨国公司进入中国市场后，它们在资金、技术、人才和市场经验等方面有巨大的优势，和我们刚刚发展起来的弱小企业不在一个起点上。由于标准竞争的特殊，跨国公司天然地占据了垄断地位，这会对我们的经济利益造成巨大损失。从现实情况看，在ICT产业反垄断的尺度要从严。比照国外标准，对任何一种产品的市场份额都做出最高限制，而不必太理会所谓的"保护创新"的观点。这样做有几个好处：一是可以防止技术标准被某一家企业完全控制；二是可以为国内企业在该领域生存和发展乃至赶超创造条件；三是即使国内完全无法提供的技术，采取反垄断措施后，保证产业链顶端标准提供者不止一家，这有利于国内企业采取策略行为，改变其在低端、被压榨的局面。

因此，政府必须防止标准形成中的"一家独大"现象。政府除了通过立法防止一家企业利用标准独占市场外，在标准竞争中需要扮演"离岸平衡手"的角色，协调欧美或者中外标准间竞争的态势。欧盟法院最近对微软的判决和处罚就有这种"平衡作用"。

(6) 适度调整知识产权保护的重点和力度。标准竞争事实上是一种内含知识产权的竞争。在"代码即将取代法律"的时代，知识产权的重要性不言而喻。自从加入WTO之后，中国承诺了一个比较高的知识产权保护水平。富田彻男认为，知识产权制度和一个国家的历史背景、市场结构等密切相关，其权利义务应该与该国研究开发的状况相称。对比一些发达国家的知识产权保护历程和我国ICT产业整体所处的技术水平，无视我们的实际创新水平和积累，强调保护知识产权，会丧失通过技术扩散、模仿、创新而发展的机会。特别在标准战这种"赢者通吃、跑马圈地"的领域，后发者更需要生存空间。采取过于严格的知识产权保护，不利于技术吸收和技术外溢，提升我国整体的技术水平。因此利用政府强势地位，为企业争取相对宽松的知识产权竞争环境就显得非常必要[FIAS2007]。

10.4　从华为中兴海外受阻谈我国ICT供应链发展的应对

10.4.1　华为中兴再遭美国国会调查

2012年10月8日，美国众议院情报委员会提交的《关于华为及中兴通讯引发的对美安全威胁问题》调查报告。报告称，华为和中兴通讯可能对美国国家安全构成威胁，应当禁止其在美国的收购及交易活动，如表10-1所示。

调查报告显示，中国电信设备制造商华为未能充分解释在美商业利益、与中国政府的关系，也未很好地配合为期一年的调查，因此在美国的关键基础设施中使用华为提供的产品，可能会危害到美国的核心国家安全利益。美国众议院情报委员会在报告中建议，美国方面应通过美国海外投资委员会阻止涉及上述两家公司的并购活动。此外，美国政府应避免使用这两家公司的设备，美国企业也应寻找可替代华为与中兴通讯的电信设备供应商。这些没有根据的指控正在损害中国公司进入美国市场。

表 10-1 众议院特别情报委员会对华为中兴的五条建议

1	国家战略	美国应当对于中国电信公司在美国电信业的持续渗透现状保持怀疑的眼光。对于这个威胁，美国情报机构必须保持警惕和集中。情报局要积极地采取措施，保证私人企业能够尽可能地知晓这个威胁
2	外包安全	督促已经与华为或中兴设备或服务建立业务联系的美国私人实体部门，关注自身长期的安全危害问题。从各种以掌控的信息来看，华为和中兴不能够作为一个不受国家影响的独立力量，因此它会对美国基础设施构成威胁
3	安全采办	外国在美国投资委员会上的收购或兼并，一旦威胁到美国国家安全利益的，应立即针对其采购协议进行安全审议。美国政府系统，不应该使用华为或中兴通讯的设备，包括零部件
4	立法和标准	在美国国会的管辖范围内，相关部门应积极调查中国电信行业在贸易中采取的不公平做法，特别是中国继续提供财政支持的重点企业。美国国会的司法委员会应该考虑可能的法律条款，以明确应对由于政府利益相关联的通信公司对美国所造成的威胁
5	对中国的建议	中国企业应尽快遵循更加开放、透明的贸易要求，采用第三方评估形式提供出一份独立一致的财务信息和网络安全审查报告。遵守美国的法律标准生产，及所有的知识产权法律和标准

华为中兴两家企业均回应称相关指控毫无根据，忽略了目前全球通信市场的技术和商业现实。中国商务部新闻发言人沈丹阳 10 月 9 日表示，美国国会的调查报告仅凭主观猜忌和不实依据，就以国家安全为由，对中国进行无端指控，排斥中国企业在美开展正常经营和参与正当竞争，中方对此表示严重关切和强烈反对。11 月 11 日，中国商务部部长陈德铭在中共十八大会议期间称，美国政府正在用“冷战思维”对待中国电信设备制造商华为，担心该公司会对其构成安全威胁。“如果你将我看成是特洛伊木马，那么我又该如何看待你呢？如果美国人能够换位思考，那么他们就会发现这种逻辑并不符合他们的利益。”

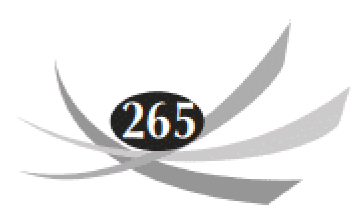
据路透社 10 月 17 日的报道，一项由美国白宫委托、历时 18 个月的调查显示，没有证据显示华为公司在美国从事任何间谍活动。但白宫国家安全委员会发言人对这一报道拒绝置评。华为公司发言人则表示，公司对这一调查并不知情，但对华为未从事间谍活动的调查结果毫不意外。

虽然白宫委托的调查并未发现任何实质性证据，但该调查依然声称，华为产品存在被黑客利用的系统漏洞，未来可能对美国国家安全构成威胁。但调查并未明确这些系统漏洞是华为刻意设计的，还是单纯的系统缺陷。

纵观《由中国电信公司华为和中兴通讯所带来的美国国家安全问题的调查报告》，充分体现了美国的国家政策在信息安全方面的延续性，特别强调了电信供应链问题——电信供应链漏洞的国家威胁是应最优先考虑的重点因素。它所关注的是整个供应链的安全，而不仅仅是关键基础设施。

10.4.2 华为中兴海外历年失利事件

尽管目前不同国家针对华为中兴的态度有所不同，但过去数年来，像华为中兴这样的



企业的“走出去”之路历尽坎坷。以下主要对中兴华为海外市场失利事件做了简要总结。

思科在 2003 年 1 月对华为提出诉讼，指控华为侵犯思科知识产权。华为为避免争议，修改了指令界面、用户手册、帮助屏和部分源代码，停止销售有问题的产品，同意只在全球出售修改过的新产品。2004 年 7 月，思科公司放弃了对华为的版权诉讼。

华为 2005 年 3 月时向印度外资促进署(FIPB)提交了一份投资 6000 万美元在印度建厂的计划，但由于受到印度内政部的强烈反对，印度内政部以“安全危险”为由，禁止华为掌握印度的战略电信网络。但来自印度政府内部的消息称，印度通信部是支持华为的，因为此举能够促进能够提高印度国内的生产力，并使印度公司获得由印度本土制造的廉价电信设备。但是在一些敏感问题上，每个印度政府部门都有着自己的看法，因此印度外资促进署被迫暂缓批准该项目。

华为、贝恩资本 2007 年 9 月提出 22 亿美元购 3COM，华为将持 16.5%股份。11 月，美国情报部门向美国海外投资委员会提交的一份威胁评估报告，称贝恩资本和华为联合收购 3COM 交易对美国国家安全造成了威胁。12 月，COM 亏损巨大，称已接受贝恩资本和华为收购报价。

2008 年 1 月，贝恩资本联手华为收购 3COM 一案在美国遭延期审查。2 月，华为贝恩投资 22 亿美元收购 3COM 案遭美国政府否决，华为贝恩资本撤回收购申请。2008 年 3 月，贝恩资本打起退堂鼓，宣布退出收购，华为并购 3COM 彻底告吹。

2009 年 12 月，出于国家安全考虑，印度国有电信运营商 BSNL 单方面取消给予华为的 20 亿美元采购订单。BSNL 一位高管表示：“由于订单是在双方经过详细谈判后签订的，因此不会接受附加条件。作为一家国有企业，我们不接受附加条件。”该高管决绝透露华为提出的条件内容。同月，印度政府向中兴华为的同步数字传输设备(SDH)征收高达 50%的临时反倾销税。印度海关决定对原产于中国的同步数字传输设备(SDH)征收临时性反倾销税，中兴、华为等国内龙头企业首当其冲，分别被征收产品进口价格 236%、50%的反倾销税。由于 SDH 产品占整体营收比例较小，中兴、华为在印度市场暂未受太大影响，但负面效应或会阻碍两家企业在海外市场的扩张。

2010 年 6 月 30 日，欧盟委员会宣布对从中国进口的无线网卡同时发起反倾销和保障措施调查，涉案金额达 41 亿美元。该案是欧盟史上对华反倾销金额最大的一次，也是欧盟首次对中国产品同时发起反倾销调查及保障措施调查。受影响最大的无疑是“双子星”华为和中兴——位列全球数据上网卡制造前两位，分别占有约 40%和 35%的全球市场份额。欧盟委员会在其官方公报中称，欧盟委员会在接到比利时无线网络设备生产商 Option 的投诉后认为，存在初步证据支持发起反倾销调查。Option 公司同时请求对从中国进口的无线网卡实施强制性的海关注册登记，从而将来一旦决定征收反倾销税，将可以追溯适用于已经登记并进口的产品。Option 公司是欧盟境内唯一一家生产同类产品的企业。一旦投诉成立，中国无线网卡单位产品将被征收超过 60 欧元的反倾销税。

7 月，出于国家安全问题考虑，华为被列入印度运营商网络设备采购黑名单；同月，受国家安全问题影响，华为竞购摩托罗拉网络基础设施部门、美国私有宽带互联网软件提供商 2Wire 失败。在这两宗交易中，有关华为能否争取到监管机构批准的严肃问题，均在竞标过程中起到一定作用，迫使华为提出较高的溢价。这两宗交易都必须获得美国外国

投资委员会(Committee on Foreign Investment in the United States,CFIUS)的批准,这是一个从国家安全角度出发、审议外资收购的跨部门小组。下半年,受国家安全问题影响,华为参与美国第三大电信运营商 Sprint Nextel 网络设备招标受阻,受到“国家安全”因素影响,尽管华为和中兴通讯的出价低于阿尔卡特朗讯、爱立信以及三星,美国运营商 Sprint Nextel 仍会将华为和中兴通讯排除在最近一次数十亿美元采购大单之外。美国国防部和部分立法者一直担心,让华为和中兴通讯的基础设备进入美国电信网络中,可能会给美国国家安全带来威胁。

2011 年 2 月,受迫于国家安全担忧,华为放弃收购美国公司 3Leaf Systems 特定资产。2 月 11 日,华为公司接到了美国外国投资委员会通知,建议“按照其提出的条件撤回审查申请,并撤销对 3Leaf 交易”。根据美国当地相关法规,该项交易仅涉及部分知识产权的购买,而非公司收购,无需提交美国外国投资委员会审批。华为最终迫于压力,放弃收购。

由于美国方面对于进入本国市场的外国电信设备商,有着严格的测试和设限,因此,通过并购当地公司“曲线”打开美国市场,成为本土设备商突破北美市场的策略首选。但来自美国外国投资委员会对于以安全为由的审查,却令这种路径屡屡受挫。

2012 年 4 月,美国议员以国家安全为由,反对华为竞标美国第六大无线运营商 Cellular Corp. 4G 网络建设合同。10 月,美国政府以国家安全为由,禁止华为参加美国“公共安全 700-MHz 示范网络”项目竞标。

2012 年 3 月,澳大利亚政府以“国家安全”为由禁止华为参与 359 亿澳元的全国宽带网络(NBN)项目。澳大利亚政府以担心“来自中国的网络攻击”为由,禁止华为技术有限公司对数十亿澳元的全国宽带网设备项目进行投标。澳方禁止华为投标的理由主要是华为的总裁任正非曾是中国人民解放军军人,并且从不接受媒体采访。澳方同时认为华为与中国政府“有关联”。澳大利亚司法部长罗克松(Nicola Roxon)的发言人在一份声明中说,“全国宽带网络”(National Broadband Network)是澳大利亚历史上最大的国家建设项目,也将成为澳大利亚信息基础设施的骨干,因此,作为政府重大战略投资,我们有责任竭尽所能保护该网络及网络上传输信息的完整性。声明还说,这与澳大利亚政府确保该国广泛意义上关键基础设施的安全和抗打击能力的做法是一致的。“全国宽带网络”计划达到的数据传输速度为每秒 100MB,按计划该网络将于 2020 年完工。

9 月,华为、中兴参加针对中国电信企业可能威胁美国网络基础设施安全的听证会。美国众议院情报委员会本月针对中国电信企业可能威胁美国网络基础设施安全一事举行听证会,邀请了中兴通讯董事长侯为贵、华为公司美国董事长胡厚昆出席该听证会,而该听证会的目的是了解这两家企业与中国政府的关系,以及其他相关事宜。中兴通讯内部人士表示,中兴通讯在美国并没有大规模的工程项目,只是与一些小运营商有合作,在美国市场所占份额较小,因此美国会对其安全质疑并无道理。10 月 8 日,美国会众议院情报委员会发布报告称华为中兴威胁国家通信安全美国众议院情报委员会提交的《关于华为及中兴通讯引发的对美安全威胁问题》报告称,华为和中兴通讯可能对美国国家安全构成威胁,应当禁止其在美国的收购及交易活动。此报告在业内引起轩然大波。10 月 12 日,思科指责华为窃取机密商业文档。思科表示,华为对 2003 年两家公司之间的专利

侵权纠纷做出了错误的表述，思科因此公布了此前机密文档的部分内容。思科通过公司法律总顾问钱德勒(Mark Chandler)的博客公布的文件片断中称："标注和间距的精确，不仅说明华为获得了思科的代码，而且表明思科的代码是以电子方式复制并嵌入到华为的代码中。"而华为曾多次表示，思科的说法有失公允，因有争议的源代码是华为从第三方获得的。

2013年2月1日，美国国际贸易委员会(ITC)宣布，针对中兴、华为、三星、诺基亚4家公司的网络设备，可能侵犯到美国本土公司专利权，开始发起联合"337调查"。ITC声明显示，涉案产品主要是关于3G和4G的移动无线设备。根据有关程序，ITC在启动"337调查"后，须在45日内确定终裁的目标时间，并尽快完成调查，通常案件需要在一年内做出裁决。一旦被裁定违反了《1930年美国关税法》第337条款，ITC将发布相关产品的排除令和禁止令。这意味着涉案产品将彻底丧失在美国市场销售的资格。不少业内专家和学者认为，"337调查"违背了世贸组织规则，属于一种应该摒弃的贸易保护主义行为。中国商务部也多次表示，希望美国政府恪守反对贸易保护主义承诺，共同维护自由、开放、公正的国际贸易环境，以更加理性的方法妥善处理贸易摩擦。

10.4.3 其他国家对华为中兴的态度

1. 加拿大：启用安全特例条款或狙击华为

继美国对华为、中兴发起狙击战后，加拿大可能成为下一个接棒者。

10月9日，加拿大一位政府高官暗示出于国家安全考虑，政府的通信系统可能不会使用华为设备。目前，有充分的理由担忧，欧洲国家、印度等不排除跟风排队或处于观望之中。有业内人士向《每日经济新闻》记者表示，华为、中兴面临的狙击波正呈现出扩大化迹象。

美国国会这份报告的作者之一、马里兰州民主党众议员鲁佩茨贝格在一份声明中说："根据我们的调查，加拿大同样面临风险。"由此，他建议美国和加拿大实现信息共享。

与此相呼应，加拿大总理哈珀的发言人在新闻发布会上表示，加拿大已启用了国家安全特例条款，使其在不违背国际贸易义务的情况下，可区别对待那些被认为风险过高，而不能参与政府电话、电子邮件和数据中心服务网络建设的企业。

根据这些条款，加拿大政府可对一些供应商实施歧视性政策，而不违反贸易公约。加拿大政府在发送给高科技企业的一则通知中称，加拿大政府采取这一行动的原因是对网络安全威胁的严重担忧。

而上述言论被外国媒体解读为"加拿大暗示会排除华为参与政府通讯网络建设"。让人担忧的是，后续可能对华为、中兴采取狙击行动的加拿大，也许并不是这次狙击波的最后一个接棒者。

2. 英国：监管机构调查华为称与美国国会报告无关

2012年10月12日，据英国媒体报道，英国议会情报和安全监管部门正在对华为进行调查。美国和欧洲目前都在担心，来自华为的通信基础设施会带来安全威胁。

华为在英国的业务已非常成熟，并且是英国最大电信运营商BT的合作伙伴。自2005年以来，华为就开始帮助升级网络。上月，英国首相卡梅隆会见了华为创始人任正

非，对华为表示了支持，并欢迎华为对英国的10亿英镑投资。

英国议会该委员会主席马尔科姆·列夫金德（Malcolm Rifkind）表示，早在美国国会的报告发布之前，该委员会就开始关注华为与BT之间的关系。他表示："华为的问题可以追溯至两三年前，当时美国和澳大利亚，以及其他一两个国家都表示了担忧。"

他同时表示："外界对华为尤为关注，因为华为是一家重要的中国公司，而创始人出身于中国解放军。因此外界质疑，华为是否真的独立于中国政府。"

该委员会尚未要求华为提供证据。华为表示，自11年前在英国设立首个办事处以来，一直遵循英国的监管规定和程序。华为一名发言人表示："我们与英国政府保持经常的联系，欢迎各种讨论和提问。"

BT也表示，与华为的合作关系完全合乎法律。该公司发言人表示："在使用华为设备方面，BT采用了风险管理手段。与英国政府类似，我们也认为没有必要因为美国的报告而改变我们的立场。"

该发言人还表示："BT的网络拥有强大的安全控制和内建的恢复能力。我们与每家供应商和政府密切合作，进行严格的审查，确保不存在网络安全问题。"

华为两年前在英国设立了信息安全评估中心，由一些符合安全要求的员工测试公司的硬件和软件，确保设备能抵御各种信息安全威胁。英国政府表示，这一信息安全中心确保了英国电信网络的安全性。

英国内阁一名发言人表示："评估中心很明显与英国政府的信息安全专家紧密合作，这帮助我们确认，来到英国的设备符合我们的标准。"不过列夫金德表示，该委员会将关注为何华为需要设立这一信息安全中心，该中心如何运作，以及能提供什么样的结论。该委员会的报告将于今年底之前被提交给英国首相。

3. 德国：各大电信运营商表示信任华为和中兴

美国国会针对华为和中兴调查的报告发布后，德国《明镜周刊》对德国运营商以及安全专家进行了采访，该国几大电信运营商均对与华为和中兴的业务合作表示信任。

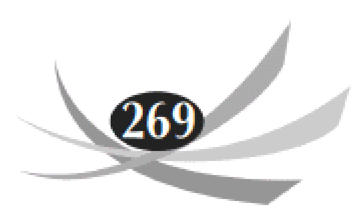
该刊认为美国国会担心间谍活动，并警告称不要与华为和中兴通讯这两家中国公司进行合作。但是在德国，这两家科技公司的业务却进展顺利：他们参与了该国超高速LTE无线网络的建设。

美国国会情报委员表示这是一场噩梦。"美国应该继续用怀疑的态度来对待中国电信设备公司进入美国市场。"这份关于华为和中兴公司的60页最终调查报告中写道。这场噩梦可能是：安装有中国设备的有线和无线网路的转换站，可能会被用于监视和消息窃取。报告称，华为和中兴存有安全风险。

在这份报告中，美国公司明确被劝阻继续与华为和中兴进行业务合作。但是在德国，所有主流电信运营商都在与这两家中国科技公司进行合作。

"被指控的活动没有具体证据"。华为公司副总裁William Plummer对美国国会的指控进行了回应：他否认了调查结果，并保证华为公司的"完整性和独立性"已经"被近150个市场所熟知"。

华为和中兴同样被德国市场所熟知。例如，两家公司都在帮助发展涉及全部德国移动运营商的超高速LTE无线网络。



在追问沃达丰时，他们表示“对两家公司表示信任”并认为“没有理由不这么做”。“关于被指控的活动并没有具体证据来证明，同时也没有关于宪法保护部分的可疑迹象。”沃达丰表示“在自己的网络中建立了自己的安全系统”。

华为在英国甚至建立了一个安全中心，地方当局可以在此检查他们的组件。这个安全评价中心(Security Evaluation Centre)位于英国办伯里，从2010年设立至今。在该国通过与联邦信息安全办公室(BSI)合作一个类似的中心也同样在考虑中。BSI关于这个问题上的声明仍然待定。

O2与华为进行了合作，对此，O2表示合同本身就约束了供应商“必须遵守德国法律并满足最高安全标准”的要求。此外，O2公司也有自己检测网络部件的安全程序。

德国电信证实，华为和中兴提供了“固网和移动网络的不同组件”。然而，这些产品“通过了我们的测试，满足我们的要求”。“不符合我们安全需求的技术，我们是不会采用的。”德国总部采用了华为和中兴的设备，但是“T-Mobile美国则未采用这两家公司的任何设备。”来自美国国会的警告对电信领域而言确实是“非常严重的”，但是“我们并未在各种各样的产品中发现任何漏洞的具体证据。”

事实上，美国国会的报告并不具体，投诉涉及更多的遗漏之处。问题并没有得到圆满解决，也未能平息担忧，(华为、中兴)与中国政府、军队以及情报机构之间可能存在的关系也未充分披露。

同样也有更加具体的指控，但是与间谍网络没有直接相关，而是其他的“犯罪行为”，例如贿赂或是使用盗版软件系统。中兴同样也被指控偷偷向伊朗出售产品，违反了联合国的制裁。同时，华为也被怀疑存有类似举动，但是显然并没有任何具体证据。最近，美国网络设备商思科系统因国会报告宣布停止与中兴的商业合作，中兴则否认曾将思科的元件卖给伊朗。

一位德国安全专家在夏天的一次会议上提出，采用华为的产品需要当心——即使最初是因为其他原因。柏林安全公司Recurity Labs的负责人Felix Lindner曾展示过华为一个路由器的安全漏洞。在拉斯维加斯的Defcon黑客会议上，他与一位同事展示了通过这一安全漏洞，黑客很容易侵入计算机系统，从而控制设备。“软件安全和代码质量低于平均水平”，Lindner说：“我不希望德国政府网络采用华为的设备，因为你无法信任它，这实在是太糟糕了。”

这位安全专家也无法判断安全问题是否本身就存在坏的意图。“区分无心之举和恶意行为几乎是不可能的。”

关于美国指控的间谍罪，他则不愿发表评论。“到现在谁都没有发现过后门，这仍然只是推测。”他表示。然而，他也指出，如果产品漏洞如此明显的话，那么根本无需黑洞，黑客们也能轻而易举地侵入。

4. 欧盟：欧盟推迟华为中兴贸易案：欧洲厂商不愿投诉

2012年10月10日消息，欧盟委员会已经推迟了针对华为和中兴通讯这两家中国电信设备制造商的一项贸易案，从而缓和了欧盟与中国之间的紧张关系。与此同时，这两家公司在美国也同样面临审查。这两家公司在出售电信设备方面已取得了更大的成功，在这一市场上有关价格的担忧情绪要比安全性担忧更强烈。据欧盟外交官和贸易专家称，

华为和中兴通讯的欧洲贸易案很可能会被推迟到明年中期。

欧盟贸易委员卡莱尔·德古特(Karel De Gucht)目前正在搜集相关证据,以便发起反倾销或反补贴调查,但爱立信和阿尔卡特朗讯等欧洲生产商并未提出投诉,因而阻碍了他为此付出的努力。在通常情况下,生产商提出正式投诉是调查程序的前提。分析师称,欧洲电信设备厂商将不愿切断自己与中国市场的联系,原因是这一市场上的电信设备需求正在增长。

中国是欧盟第二大贸易伙伴,仅次于美国,而欧盟则是中国最大的贸易伙伴。据预计,欧盟与中国今年的贸易总额将创下5000亿欧元(约合6430亿美元)。尽管如此,双方之间的关系仍很紧张。德古特曾抱怨称,中国方面的补贴严重扭曲了市场竞争。欧盟怀疑,中国生产商正在通过人为压低价格的方式损害欧盟电信设备提供商,这些公司至少有部分资金由来自于中国政府的数额庞大的信用额度提供支持。

路透社的一名证人称其看到过来自于一家中国电信设备制造商的投标,内容是更换一家欧洲运营商的全部网络,却不收取任何费用。德古特在今年5月表示,欧盟委员会正在考虑主动发起一项诉讼案,无需业内公司提出投诉。该委员会上一次主动发起贸易诉讼案是在1997年针对印度发起的。

贸易专家称,这种诉讼案将令欧盟十分尴尬,原因是欧盟委员会看起来将既是申诉方,同时又是判决者。而且,欧盟委员会仍需得到欧盟生产商和欧盟成员国的合作,原因是需要它们对该委员会的提议进行投票才能征收关税。一名欧盟贸易专家表示:"很明显,许多成员国都不支持。"

此外,欧盟委员会还希望暂停另一项调查,这项调查是在上个月发起的,原因是其怀疑中国生产商正在欧洲市场上倾销太阳能面板。虽然这项调查是在欧盟公司发起投诉后展开的,但仍旧受到来自于中国的警告。

贸易专家和外交官称,预计欧盟委员会正在等待中国方面的回应,随后才会发起一项电信贸易案。而且,欧盟委员会可能正希望太阳能面板贸易案能给中国方面带来深刻印象,表明自身将严肃处理倾销和补贴问题的立场。贸易专家称,如果在明年6月以前不采取任何行动,则欧盟将对中国太阳能面板厂商征收关税,而且很可能主动发起针对华为和中兴通讯的贸易案。

5. 新西兰:为与华为合作辩护

在美国国会委员会警告称与中国电信业巨头华为公司进行业务合作将带来间谍活动隐忧之后,新西兰政府为自己与华为达成的合作进行了辩护。华为已经与新西兰超高速光纤有限公司(Ultrafast Fibre Ltd)达成了合作,为其在怀卡托、丰盛湾、塔拉纳基和旺加努伊地区超高速宽带的推出提供技术。2012年3月,新西兰总理John Key曾表示对安排感到满意。作为反对党的工党和绿党表示政府不应该这么快就放松警惕、解除担忧。工党议员David Cunliffe希望对华为如何参与了宽带计划进行独立调查,同时他想知道政府如何来保证这家公司是安全的。绿党技术发言人Gareth Hughes表示政府需要审视美国的报告。

通信部长Amy Adams则回应表示,反对党们"对公众造成了非常大的现状误导","事实上,华为参与了超过100个国家的通信工程,同时全球数十亿人口都在使用他们的



技术。”她在一份给 AAP 的声明中表示。“政府非常重视网络安全,并致力于与运营商和供应商一起保护新西兰电信网络的完整性和安全性。”

华为同样是新西兰的移动运营商的合作伙伴。它建造和支持 2degrees 的移动网络,建造了沃达丰的固定宽带网络,并为两家公司提供了手机。

10.4.4 华为中兴海外扩张受阻的警示与对策

此次纠缠了月余的华为中兴事件又被称为“安全门”事件。近期,有报道显示,中国联通等运营商开始替换思科核心设备,来自中国市场的反击,极有可能扭转华为中兴在美国市场的命运。而也有最新披露的信息称,华为中兴在美国遭遇不公正待遇的幕后推手,正是其最大的竞争对手,美国思科。据媒体报道,十余年来,思科为阻挠竞争对手在美发展,系统性的游说支出高达一千多万美元。同时也为中国通信企业的国际化上了极具意义的一课。

华为中兴“安全门”带来的反思是深刻的,总结中兴华为在海外市场开发过程中的种种事件,上至政府及行业协会,下至企业自身,均呈现多处痛点,在中国信息通信企业日益强大,进入国际市场的今天,积极应对危机,抹平痛点,是必需的,也是必要的。

1. 将信息安全提至国家战略层面

继陆地、海洋、天空和太空之后,战争已经进入了第五空间:网络空间。美国总统奥巴马已经宣布,美国的数字化基础设施属于“国家战略资产”,并任命微软的前安全总管霍华德·施密特(Howard Schimidt)作为网络安全总指挥。2010 年 5 月,五角大楼成立了一个新的网络司令部(Cybercom),担任领导的是国家安全局局长基思·亚历山大(Keith Alexander)将军,他的任务是开展“全方位”行动——以保卫美国的军事网络和攻击他国的系统。

负责反恐和网络安全的白宫前幕僚理查德·克拉克(Richard Clarke)在他的书中设想了十五分钟之内造成的灾难性破坏。计算机病毒让军方的 E-mail 系统瘫痪、造成炼油厂和输油管道爆炸、空中交通管制系统瘫痪、货运和城市铁路列车出轨、金融数据被涂改、美东电网断电、轨道卫星运转失控等灾难性事故。随着食物紧缺,资金链断裂,整个社会很快分崩离析。最糟糕的是,攻击者的身份一直成谜。

由网络安全公司 McAfee 发表的“虚拟犯罪报告”称,这一切已经从科幻小说变成了现实。该报告警告说,网络攻击对国家的基础设施有“破坏性的”影响,电网、供水系统和金融市场都处在危险之中。

因此,近年来,美国对网络安全的研究和实践已经处在全世界非常前沿的位置。“所以,华为中兴事件不是孤立的,而是美国对网络安全、网络战争的持续性思考和实践背景下做出的动作。华为中兴事件不仅仅是一种惯性的主动防御也更具有美国先发制人的意味。”业内专家分析。

美国已经成为最为积极和深度使用网络战的国家。据了解在过去数年伊朗的核工业网络和核心设施持续遭遇到来自网络病毒的攻击和破坏便是美国主导的。2012 年 6 月,美国和以色列官员最终承认和证实,双方对伊朗采用了网络战武器(Stuxnet、Duqu、Flame 病毒)。Stuxnet 病毒又称为“震网”病毒,一直潜伏在伊朗核设施中所使用的西门

子设备，该病毒已经辗转侵入核设施离心机的工业软件，长达一年没有被发现，感染了伊朗至少6万台计算机。

安全专家分析，“震网”病毒不像普通的病毒木马，需要非常专业的专家和资金投入才能研发出来，可以说是美国精心制造的网络武器。专家提醒，美国可能还拥有更多的网络武器，有些可能早已潜伏进美国之外的各种设备中，等待唤醒。

而我国一旦遭遇“网络战”，或将造成非常严重的后果。因为我国的网络基础设施大部分依赖思科、微软和英特尔美国企业提供。据了解，思科占据了中国电信163骨干网络70%以上的份额，把持着163骨干网所有的超级核心节点和绝大部分普通核心节点，更是占据了中国联通169骨干网80%以上的份额，把持着所有超级核心、国际交换节点、国际汇聚节点和互联互通节点。与此同时，我国的计算机系统等设备几乎全部采用英特尔的芯片，而操作系统和办公软件则依赖微软提供。

更严重的是，在密码后门、加密算法及协议设计等方面，思科IOS系统却有着鲜为人知的缺憾和威胁。2010年的黑帽大会上，IBM互联网安全系统公司的研究人员Tom Cross论证说，黑客可轻易地利用思科IOS操作系统中的后门，对路由器进行管理配置，进而将整个网络置身于未知的风险中。

而且在现网思科路由器产品中，使用的乃是上世纪70年代的加密算法DES(数据加密标准)。这种算法是1972年由美国IBM公司研制确定的，并已经被多次证明不再安全，即使一台普通的PC机，也能够在10分钟内完成DES算法的破解。

不仅如此，思科在协议报文的认证中，使用的也是DES算法，而这种极易被破解的算法，很容易造成用户密码的泄露，进而对用户安全造成威胁。

带有如此硬伤的网络设备，正在维系着中国现网的运转，由此不难想象，我国网络安全已然到了紧要时刻。

因此，华为中兴“安全门”事件也发出警示：我国政府必须把信息系统安全问题提到关系国家安全和国家主权的战略性高度。

2. 加强信息安全立法工作

美国是世界上最早建立和使用计算机网络的国家，也是信息产业发展最为迅速的国家，信息安全一直处于美国国家安全战略的高度。早在十年前美国便公布了《网络安全国家战略》以及《确保信息安全的国家战略》，确定了3个战略目标和5项优先行动，并通过为信息安全立法，来完善保障信息安全法规体系。

近年来，美国尤其重视信息安全，相继制定了《信息自由法》、《总统档案法》、《联邦信息资源管理法》、《国家信息基础设施保护法案》、《反电子盗窃法》、《计算机犯罪强制法》等一系列法律法规，以确保国家安全。

而我国的信息安全立法相对于美国则远无法望其项背，无论是重要信息系统和工业控制系统，还是个人信息安全，安全状况均堪忧，国家经济发展和产业安全面临挑战，在贸易保护主义更加显现出来的背景下，我国应该要借鉴美国的商业安全检查体系，在经济安全和产业安全体系上做出更多的努力，法规和各方面运作等要尽快完善。

3. 建立对国外设备的安全审查制度

可以看到，网络信息安全已经成为国家安全的核心内容和关键要素，并日益成为整个



社会安全的基础。因此，专家呼吁，保障通信安全应建立审查制度，从设备采购为始，对设备进行严格的审查，以长期监管维护为终，进行系统的定期审查，才能保障中国网络信息安全。

目前，华为的网络设备也被大规模运用在欧洲主流运营商中，便是基于华为和政府以及运营商之间的信任。

例如，在英国，政府与华为达成协议，采取了初步措施来解决问题，建立了拥有独立管理权的信息安全评估中心（CSEC）。CSEC 独立管理对华为在英国部署的电信基础网络设备和软件的安全评估，并将评估的结果提供给英国的运营商和政府。英国政府的目的是试图减少华为在英国关键的电信基础网络中部署的产品带来的威胁。

微软为了表明系统的安全性，也与多个国家的政府签署源代码授权查看条约。例如，我国早在 2003 年便成立了中国信息安全产品测评认证中心源代码查看实验室，通过协议规定的方式查看微软公司 Windows 操作系统的源代码，进行信息安全方面的研究。

历史上几个经典的"后门"行为，都发生在美国公司身上。据报道，美国惠普公司有一款网络打印机，能在打印者不知情的情况下，将打印过的文件复制下来通过网络发送出去。现在我国普遍使用的微软公司 OFFICE 软件，也存在明显的"后门"。Rixler 软件公司在网上正在出售破解 OFFICE 软件密码的程序。而分析该公司破解文档"open"密码的方式可以发现，他们并不是按照常规的暴力破解方式获知密码，而是将密码旁路掉，使得文档成为没有密码的文档。这就好比他们不是把密码柜的密码给猜测出来，而是直接把带有密码的柜门给卸了下来。显然，只有 OFFICE 留了旁路文档密码的"后门"，才会有这样的结果存在。

而中国消费者最熟悉的一次"后门"事件，则是微软 Windows 将盗版软件黑屏的事件。2008 年 10 月，微软称其为了打击盗版，通过系统升级强制安装鉴别软件，并每隔 60 分钟将"盗版系统"桌面强制修改为黑屏。也就是说，虽然微软告知用户在下载更新，但是多数用户并不知道下载来的更新软件到底是用来做什么的。如果微软有意欺瞒，我们也可能在系统升级时下载安装泄露个人信息的软件。这充分暴露出我国信息安全存在风险。

此次美国质疑华为、中兴留"后门"，从另一个角度也启发了我们：关注信息安全，应该从审查境外信息产品入手。境外企业不受我国法律制约，我们必须防患于未然。北京邮电大学前校长方滨兴院士建议，中国政府应尽快成立国家信息安全审查委员会，以保障中国国家和公民的信息安全不因信息技术产品的引入而受到威胁。

中国在电信设施建设方面展示了足够开放的姿态，但是另一方面也显得缺乏清晰的安全意识与防范措施。中国现在仅有的一些测评中心，只能测评信息安全产品本身的适用性，不能测评网络产品所引发的安全性。更重要的是，在一些大的方面，比如对一些产品在重要部门中使用或在我国大规模使用，也需要一个机构来牵头进行风险评估。

4. 企业提高安全意识

提升从企业管理到产品技术的全面信息安全意识，尽管有的企业不是信息安全厂商，但是其产品担当了网络核心位置职能，就必须承担起相应的信息安全责任，并且要习惯未来更多用户对于产品信息安全的更多需求、更严要求和合理质疑。尤其要投入更大的科

研力度，进行安全机制的研发，要确保客户的安全，更获得客户的信任，因为未来，对任何客户来说，也许对安全的需求将大于别的功能需求。

10.5 ICT供应链技术新兴应用领域探索

供应链的协调运行建立在各个节点高质量的信息传递与共享的基础之上，有效的供应链管理离不开信息通信技术系统提供的可靠支持。ICT是当今世界发展速度最快、覆盖范围最广、渗透性最强、应用最广泛的高新技术，是提高生产力、促进经济增长、实现国家现代化的强大工具。目前，各国对ICT在社会发展中所起到的重要作用已达成了广泛的共识，ICT正日益成为各国国家创新与发展战略的核心。

ICT产业发展中的一个显著特点便是新技术新业务发展迅速，新技术对整个行业乃至整个社会经济的促进作用影响十分显著。信息通信技术不仅拓展了信息通信业的发展空间，也有助于向消费者提供更方便、更快捷、更丰富和更具个性化的信息服务。在技术进步的推动下，融合、转型、创新已成为当前ICT产业的整体发展趋势。

随着计算机技术、通信技术和控制技术的发展，传统的控制领域正经历着一场前所未有的变革，开始向网络化方向发展。控制系统的结构从最初的CCS(计算机集中控制系统)，到第二代的DCS(分散控制系统)，发展到现在流行的FCS(现场总线控制系统)。对诸如图像、语音信号等大数据量、高速率传输的要求，又催生了当前在商业领域风靡的以太网与控制网络的结合。这股工业控制系统网络化浪潮又将诸如嵌入式技术、多标准工业控制网络互联、无线技术等多种当今流行技术融合进来，从而拓展了工业控制领域的发展空间，带来新的发展机遇。

智能电网(smart power grids)，就是电网的智能化。从技术发展和应用的角度看，智能电网是将先进的传感测量技术、信息通信技术、分析决策技术、自动控制技术和能源电力技术相结合，并与电网基础设施高度集成而形成的新型现代化电网。

由于智能电网的研究与开发尚处于起步阶段，各国国情及资源分布不同，发展的方向和侧重点也不尽相同，国际上对其还没有达成统一而明确的定义。根据目前的研究情况，智能电网就是为电网注入新技术，包括先进的通信技术、计算机技术、信息技术、自动控制技术和电力工程技术等，从而赋予电网某种人工智能，使其具有较强的应变能力，成为一个完全自动化的供电网络。

智能电网的建设进程伴随着电力系统中数字化和信息化程度的不断提高，系统中的能量流和信息流的交换与互动亦日益频繁，最终使得未来智能电网在很大程度上将发展成一类由信息网和物理电力网构成的相互依存的二元复合网络。在此背景下研究信息网和物理网相互依存的新一代电力网络的拓扑结构特征、连锁故障传播机理、安全水平和生存能力以及相应的预防控制措施，在理论和工程两方面均具有重要意义。

10.5.1 工业控制系统供应链安全

1. 工业控制系统概述

工业控制系统(Industrial Control Systems，ICS)，是由各种自动化控制组件以及对

实时数据进行采集、监测的过程控制组件,共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统[ZS2012]。其核心组件包括数据采集与监控系统(SCADA)、分布式控制系统(DCS)、可编程逻辑控制器(PLC)、远程终端(RTU)、智能电子设备(IED),以及确保各组件通信的接口技术。目前工业控制系统广泛的应用于我国电力、水利、污水处理、石油天然气、化工、交通运输、制药以及大型制造行业,其中超过80%的涉及国计民生的关键基础设施依靠工业控制系统来实现自动化作业,工业控制系统已是国家安全战略的重要组成部分。

SCADA(Supervisory Control And Data Acquisition)数据采集与监控系统,是工业控制系统的重要组件,通过与数据传输系统和 HMI 交互,SCADA 可以对现场的运行设备进行实时监视和控制,以实现数据采集、设备控制、测量、参数调节以及各类信号报警等各项功能。目前,SCADA 广泛应用于水利、电力、石油化工、电气化、铁路等分布式工业控制系。

DCS(Distributed Control Systems)分布式控制系统,广泛应用于基于流程控制的行业,例如电力、石化等行业分布式作业,实现对各个子系统运行过程的整体管控。

PLC(Programmable Logic Controllers)可编程逻辑控制器,用以实现工业设备的具体操作与工艺控制。通常 SCADA 或 DCS 系统通过调用各 PLC 组件来为其分布式业务提供基本的操作控制,例如汽车制造流水线等。

2. 工业控制系统安全风险分析

随着计算机和网络技术的发展,特别是信息化与工业化深度融合以及供应链研究的快速发展,工业控制系统越来越多地采用通用硬、软件和协议,木马、病毒等威胁正在向工业控制系统扩散,工业控制系统信息安全问题日益突出,据权威工业安全事件信息库RISI(Repository of Security Incidents)统计,截止 2011 年 10 月,全球已发生 200 余起针对工业控制系统的攻击事件。2001 年后,通用开发标准与互联网技术的广泛使用,使得针对 ICS 系统的攻击行为出现大幅度增长,ICS 系统对于信息安全管理的需求变得更加迫切。

(1) 风险分析。工业控制系统是重要基础设施自动化生产的基础组件,安全的重要性可见一斑,然而受到核心技术限制、系统结构复杂、缺乏安全与管理标准等诸多因素影响,运行在 ICS 系统中的数据及操作指令随时可能遭受来自敌对势力、商业间谍、网络犯罪团伙的破坏。根据工信部《关于加强工业控制系统信息安全管理的通知》要求,我国工业控制系统信息安全管理的重点领域包括核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域。这些领域中的工业控制系统一旦遭到破坏,不仅会影响产业经济的持续发展,更会对国家安全造成巨大的损害。

工业系统入侵事件如表 10-2 所示。

表 10-2　工业系统入侵事件

时间	国家/地区	事　　件
1992	美国	一位前雇员关闭了雪佛龙位于 22 个州的应急警报系统,直到一次紧急事件发生之后才被发现
1994	美国亚利桑那州	Salt River Project (SRP) 被黑客入侵

续表

时间	国家/地区	事　件
1997	美国纽约	一个十几岁的少年侵入(纽约)NYNES 系统，干扰了航空与地面通信，导致马萨诸塞州的 Worcester 机场关闭 6 个小时
2000	俄罗斯	俄罗斯政府声称黑客成功控制了世界上最大的天然气输送管道网络(属于 GAzprom 公司)
2000	澳大利亚	一位工程师在应聘澳大利亚一污水处理厂被多次拒绝后，远程侵入该厂的污水处理控制系统，恶意造成污水处理泵站的故障，导致超过 1000 立方米的污水被直接排入河流，导致严重的环境灾难
2003	美国俄亥俄州	美国俄亥俄州 Davis Besse 的核电厂控制网络内的一台计算机被微软的 SQL Server 蠕虫所感染，导致其安全监控系统停机将近 5 小时
2003	美国华盛顿特区	CSX 运输公司的计算机系统被病毒感染，导致华盛顿特区的客货运输中断导致华盛顿特区的客货运输中断
2005	美国	在 Zotob 蠕虫安全事件中，尽管在 Internet 与企业网、控制网之间部署了防火墙，还是有 13 个美国汽车厂。由于被蠕虫感染而被迫关闭，50 000 生产线工人被迫停止工作，预计经济损失超过 1 400 000 美元
2006	美国哈里斯堡	黑客从 Internet 攻破了美国哈里斯堡的一家污水处理厂的安全措施，在其系统内植入了能够影响污水操作的恶意程序
2007	加拿大	攻击者侵入加拿大的一个水利 SCADA 控制系统，通过安装恶意软件破坏了用于控制从 Sacrmento 河调水的控制计算机
2008	美国	在美国国土安全局的一次针对电力系统的渗透测试中，一台发电机在其控制系统收到攻击后被物理损坏
2008	波兰	一名少年攻击了波兰 Lodz 的城铁系统，用一个电视遥控器改变轨道扳道器，导致 4 节车厢出轨
2010	伊朗	“网络超级武器 ”Stuxnet 病毒通过针对性的入侵 ICS 系统，严重威胁到伊朗布什尔核电站核反应堆的安全运营
2011	美国	黑客通过入侵数据采集与监控系统 SCADA ，使得美国伊利诺伊州城市供水系统的供水泵遭到破坏

分析可以发现，造成工业控制系统安全风险加剧的主要原因有两方面：

首先，传统工业控制系统的出现时间要早于互联网，它需要采用专用的硬件、软件和通信协议，设计上以武力安全为主，基本没有考虑互联互通所必须考虑的通信安全问题。

其次，互联网技术的出现，导致工业控制网络中大量采用通用 TCP/IP 技术，工业控制系统与各种业务系统的协作成为可能，愈加智能的 ICS 网络中各种应用、工控设备以及办公用 PC 系统逐渐形成一张复杂的网络拓扑。

仅基于工控协议识别与控制的安全解决方案在两方面因素的合力下，已无法满足新形势下 ICS 网络运维要求，确保应用层安全是当前 ICS 系统稳定运营的基本前提。利用工控设备漏洞、TCP/IP 协议缺陷、工业应用漏洞，攻击者可以针对性的构建更加隐蔽的攻击通道。

(2) 脆弱性分析。工业控制系统的安全性和重要性直接影响到国家战略安全实施，但为兼顾工业应用的场景和执行效率，在追求 ICS 系统高可用性和业务连续性的过程中，用户往往会被动的降低 ICS 系统的安全防御需求。识别 ICS 存在的风险与安全隐



患，实施相应的安全保障策略是确保 ICS 系统稳定运行的有效手段。

- 安全策略与管理流程的脆弱性。追求可用性而牺牲安全，这是很多工业控制系统存在普遍现象，缺乏完整有效的安全策略与管理流程是当前我国工业控制系统的最大难题，很多已经实施了安全防御措施的 ICS 网络仍然会因为管理或操作上的失误，造成 ICS 系统出现潜在的安全短板。例如，工业控制系统中的移动存储介质的使用和不严格的访问控制策略。
- 工控平台的脆弱性。随着 TCP/IP 等通用协议与开发标准引入工业控制系统，开放、透明的工业控制系统同样为物联网、云计算、移动互联网等新兴技术领域开辟出广阔的想象空间。理论上绝对的物理隔离网络正因为需求和业务模式的改变而不再切实可行。
- 网络的脆弱性。通用以太网技术的引入让 ICS 变得智能，也让工业控制网络愈发透明、开放、互联，TCP/IP 存在的威胁同样会在工业网络中重现。此外，工业控制网络的专属控制协议更为攻击者提供了了解工业控制网络内部环境的机会。确保工业网络的安全稳定运营，必须针对 ICS 网络环境进行实时异常行为的“发现、检测、清除、恢复、审计”一体化的保障机制。

3. 工业控制系统漏洞

(1) 协议漏洞。两化融合和物联网的发展使得 TCP/IP 协议和 OPC 协议等通用协议越来越广泛地应用在工业控制网络中，随之而来的通信协议漏洞问题也日益突出。例如，OPC Classic 协议（OPCDA，OPCHAD 和 OPCA&E）基于微软的 DCOM 协议，DCOM 协议是在网络安全问题被广泛认识之前设计的，极易受到攻击，并且 OPC 通讯采用不固定的端口号，导致目前几乎无法使用传统的 IT 防火墙来确保其安全性。因此确保使用 OPC 通讯协议的工业控制系统的安全性和可靠性给工程师带来了极大的挑战。

(2) 操作系统漏洞。目前大多数工业控制系统的工程师站/操作站/HMI 都是 Windows 平台的，为保证过程控制系统的相对独立性，同时考虑到系统的稳定运行，通常现场工程师在系统开车后不会对 Windows 平台安装任何补丁，但是存在的问题是，不安装补丁系统就存在被攻击的可能，从而埋下安全隐患。

(3) 策略和管理流程漏洞。追求可用性而牺牲安全，是很多工业控制系统存在的普遍现象，缺乏完整有效的安全策略与管理流程也给工业控制系统信息安全带来了一定的威胁。例如工业控制系统中移动存储介质包括笔记本电脑、U 盘等设备的使用和不严格的访问控制策略。

(4) 杀毒软件漏洞。为了保证工控应用软件的可用性，许多工控系统操作站通常不会安装杀毒软件。即使安装了杀毒软件，在使用过程中也有很大的局限性，原因在于使用杀毒软件很关键的一点是，其病毒库需要不定期的经常更新，这一要求尤其不适合于工业控制环境。而且杀毒软件对新病毒的处理总是滞后的，导致每年都会爆发大规模的病毒攻击，特别是新病毒。

(5) 应用软件漏洞。由于应用软件多种多样，很难形成统一的防护规范以应对安全问题；另外当应用软件面向网络应用时，就必须开放其应用端口。因此常规的 IT 防火墙等安全设备很难保障其安全性。互联网攻击者很有可能会利用一些大型工程自动化软件

的安全漏洞获取诸如污水处理厂、天然气管道以及其他大型设备的控制权，一旦这些控制权被不良意图黑客所掌握，那么后果不堪设想[GY2012]。

4. 基于终端的安全管理体系

作为国家的重要基础设施，工业控制系统的安全性对国家安全、社会利益具有重要的影响，为此工信部要求各级政府和国有大型企业切实加强 ICS 系统的信息安全管理。而与此同时，国内重要行业 ICS 系统还普遍被《信息安全等级保护》定为第三或第四级，工业信息系统的安全管理体系建设还需兼顾等级保护技术要求。国际方面，各国网络空间战略的进一步发展，国与国的防御战略已经从现实延伸到虚拟世界，网络空间更是各国未来发展战略中的必争之地。自从网络“超级武器”Stuxnet 蠕虫的出现，谁也无法保证本国的关键基础设施不会成为下一个攻击目标。

因此，传统的信息安全管理体系需要重新思考工业安全的重要性和防御策略，针对工业控制系统终端的特殊性以及 IT 信息安全的管理需求，构建基于终端的安全管理体系是现阶段满足不同环境信息安全管理需求的重要手段，如图 10-1 所示。

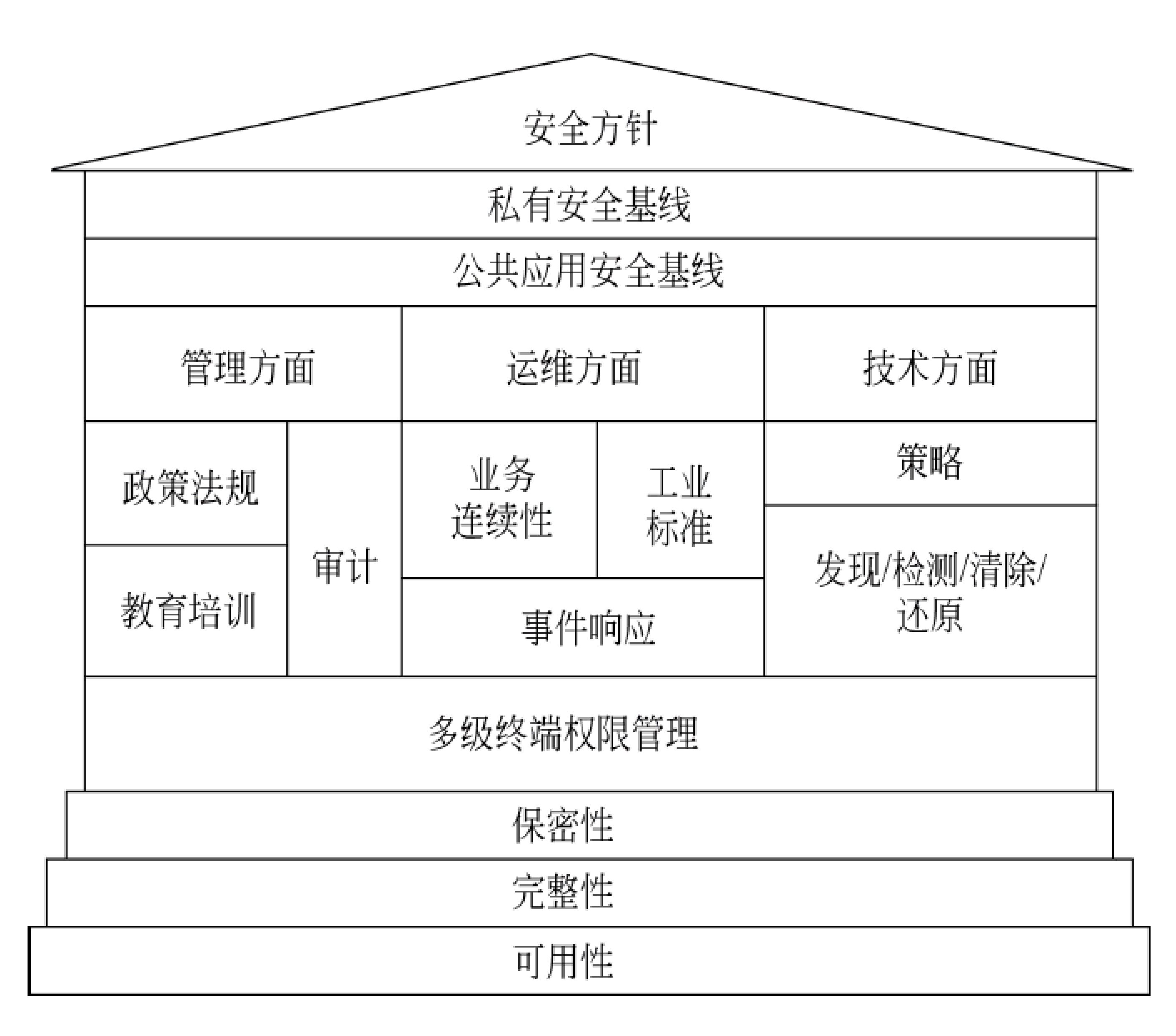


图 10-1 基于终端的信息安全管理系统

当然，无论是国家未来发展战略的要求，还是确保国家重要基础设施可用性的需要，从管理、流程、架构、设备、技术等多个角度，构建满足工业控制系统安全管理体系，不断改进并完善，是确保新时期工业控制系统和国家重要基础设施安全的最有效手段。

早期计算机与物理对象的系统集成实现了工业自动化，能够用计算机来代替人的操控等诸多工作。而网络和通讯技术的发展，计算单元和物理对象通过通讯网络的系统集成将带来更多技术上的优势和潜在利益：可以使得许多大型复杂系统如国家电网等运行更安全，效率更高；可以减少这些系统构建及其操作这些系统的费用；这些系统允许不同的子系统通过网络进行组合和集成，形成更为复杂的系统，产生新的功能，拥有更灵活和强大的能力。CPS 就是计算(computing)、通信(communication)、控制(control)与物理系统(physical systems)的集成，其核心是 3C 的融合。它具有应对环境不确定性变化的自



适应性，动态自组织重构功能及基于网络的大规模系统集成控制。CPS在物理设备和程序控制下，无缝地集成了传感器、网络、计算器和控制单元，它作为计算过程和物理过程的统一体，是集成计算、通信与控制于一体的下一代智能系统。目前对于CPS的研究正处于起步阶段，关于CPS的供应链安全问题也将得到越来越多的关注。

10.5.2 智能电网供应链安全

1. 国内外智能电网研究现状

近年来，利用现代信息技术和控制技术建设智能电网成为了各国研究的热点。美国电科院(EPRI)于2001年开始智能电网的研究。2009年美国总统奥巴马更是将智能电网的建设提升到了国家战略的高度。美国能源部(DOE)将利用信息技术对陈旧老化的电力设施进行升级。以提高供电的安全性、可靠性和能源的利用效率；降低排放水平；建立适用于可再生能源接入的控制体系，最终建成完全自动化的发电、输电、配电和用电网络。

欧洲在2006年制定了战略性的研究规划，目的是建立能够满足用户多样化电力需求，并且大量利用可再生清洁能源的，高效、经济、可靠的未来电网。

我国智能电网的研究也正在起步，预计建设以信息化、自动化、数字化和互动化为特征的坚强电网。它在技术上应该是可观测、可控制、自适应并且强壮的。较现有电网更加高效、安全、经济且清洁。

2. 智能电网的安全需求

智能电网作为物联网时代最重要的应用之一，将会给人们的工作和生活方式带来极大的变革，但是智能电网的开放性和包容性也决定了它不可避免地存在信息安全隐患。针对智能电网的运营特点，其安全需求主要包括物理安全、网络安全、数据安全及备份恢复等方面[ZN2013]。

(1) 物理安全。智能电网的物理安全是指智能电网系统运营所必需的各种硬件设备的安全。这些硬件设备主要包括智能计、测量仪器在内的各类型传感器，通信系统中的各种网络设备、计算机以及存储数据的各种存储介质。物理安全主要指保证硬件设备本身的安全和智能电网系统中其他相关硬件的安全，是智能电网信息安全控制中的重要内容。物理安全的防护目标是防止有人通过破坏业务系统的外部物理特性以达到使系统停止服务的目的，或防止有人通过物理接触方式对系统进行入侵。要做到在信息安全事件发生前和发生后能够执行对设备物理接触行为的审核和追查。

(2) 网络安全。在传统电力系统基础上，智能化的通信网络架构的智能电网应具有较高的可靠性。该通信网络必须具备二次系统安全防护方案。防护的原则是：安全分区、网络专用、横向隔离、纵向认证。根据这个原则，智能电网的通信网络可划分为4个分区：安全区Ⅰ(实时控制区)、安全区Ⅱ(非控制生产区)、安全区Ⅲ(生产管理区)、安全区Ⅳ(管理信息区)。其中，安全区Ⅰ、安全区Ⅱ和安全区Ⅲ之间必须采用经相关部门认定核准的电力专用安全隔离装置，必须达到物理隔离的强度。网络纵向互联时，互联双方必须是安全等级相同的网络。要避免安全区纵向交叉，同时在网络边界要采用逻辑隔离。信息系统网络运行过程中要充分利用防火墙、虚拟专用网，采用加密、安全隔离、入侵检测以

及网络防杀病毒等技术来保障网络安全。

(3) 数据安全及备份恢复。在智能电网中,数据安全的含义有两点:其一,数据本身的安全。即采用密码技术对数据进行保护,如数据加密、数据完整性保护、双向强身份认证等。其二,数据防护的安全,即采用信息存储手段对数据进行主动防护,如通过磁盘阵列、数据备份、异地容灾以及云存储等手段保证数据的安全。

智能电网整体的信息安全不能通过将多种通信机制的安全简单叠加来实现。除了传统电力系统的信息安全问题之外,智能电网还会面临由多网融合引发的新的安全问题。

- 感知测量节点的本地安全问题。由于智能电网中的智能设备可以取代人来完成一些复杂、危险和机械的工作,所以智能电网的感知测量节点多数部署在无人监控的电力系统环境中。攻击者可以轻易地接触到这些设备,从而对它们造成破坏,甚至通过本地操作更换机器的软硬件。
- 感知网络的传输与信息安全问题。感知测量节点通常情况下功能唯一、能量存储有限,使得复杂的安全保护技术无法应用。而智能电网的感知网络形式多样,从功率测量到稳压监控,再到电价实时控制,它们的数据传输没有特定的标准,所以没法提供统一的安全保护体系。
- 核心通信网络的传输与信息安全问题。核心通信网络具有相对完整的安全保护能力。但是由于智能电网中节点数量庞大,且以集群方式存在,因此会导致在数据传播时,由于大量机器的数据发送使网络拥塞,产生例如拒绝服务攻击等一系列安全威胁。此外,现有通信网络的安全架构都是从人与人之间通信的角度设计的,并不适用于机器之间通信。简单套用现有安全机制不符合智能电网的设备之间的逻辑关系。
- 智能电网业务的安全问题。由于智能电网中的设备可能是先部署后联网,同时又会面临无人看守的情况,所以如何对智能电网中的设备进行身份认证和业务配置就成了难题。庞大且内部多样化的智能电网需要一个强大而统一的信息安全管理平台来统一管理,否则独立化的子平台会被各式各样的智能电网应用所淹没。另外,如何在对智能电网中设备的日志等安全信息进行管理的同时,不破坏通信网络与业务平台之间的信任关系也是必须研究的问题。

3. 供应链管理在智能电网建设中的应用和策略

1) 电力企业物资供应链管理的发展趋势

构建供应链企业间的信任机制,逐步提高供应链的协同性,包括采购协同、库存协同、生产过程协同、质量控制协同、财务管理协同以及成本核算与控制协同,使整条供应链获得更大的效益;与供应链中重要的供应商建立电子数据交换系统(EDI),建立信息共享机制;物流配送须引入国外先进理念,提升物流管理的效率和效益;改造电力企业供应链业务流程,实现采购及项目管理的自动化,并构建供应链考核机制;建立健全先进信息系统,使用高水平供应链管理软件。

2) 智能电网建设过程中供应链管理难点

(1) 外围政策不确定性,影响采购准时化。电力基建项目要纳入地方市政规划,通常受到土地供给的影响,存在电力物资采购行为已经发生,而土地使用权不能及时得到批



复,使工程项目延期,影响准时采购。

(2) 由于智能电网系统在建设过程中工程量大,涉及特高压工程、智能变电站、配电自动化系统、用电信息采集系统等多个工程。电网建设周期基本集中在每年 5 月～10 月,全国电网工程的建设周期引起的采购紧张。导致供应链的传递效应,使这段时间成为电力物资采购高峰期。电力设备供应商,特别是重点供应商的产能可能在这一时间区间达到极限,致使电力物资供应紧张,使采购效率收到影响。

(3) 受到供应链上游供应商产品(原材料)价格影响,导致的采购价格波动。如 2010 年上半年,角钢、板材等设备建设材料价格的不断大幅上升与高位震荡,设备价格波动剧烈,供应商对原材料价格敏感性增强,对已经签订的供货合同产生涨价的要求,使供应链下游电网企业采购成本增加,设备供货准时性减弱。

(4) 智能电网对于关键设备的制造水平与工艺要求较高,虽然众多国际知名电力设备供应商在中国建立了合资或独资制造厂,部分地实现了本土化制造,但部分关键配件还要依赖进口,造成了配件进口成本高,物资在供应链流转时间长,进而对电网设备的维护、抢修造成影响[XM2009]。

根据目前电网企业智能电网供应链管理特征及结构分析,提出以下策略。

(1) 提升供应链管理的战略意识。鉴于在管理中主辅供应链结构及其发展状况的不平衡,建议分别采取不同的供应链管理战略及策略。对于主供应链,在今后相当一段时期保持电力行业地位的同时,应居安思危,提高自身的效率,弱化非效率垄断表现。强化市场经营意识,按照大电网之间市场开放与市场准入的规则,直面电力市场化等即将形成的竞争性市场的格局。对于辅供应链,应加强供应商管理的战略意识,对一级、二级供应商的有效管理将是降低供应链成本与风险的最直接和最有效手段,也是未来建设坚强智能电网的关键要素。高效率的供应商将是高效率的供应链管理的基础。

(2) 改善现有供应链结构。建设完善的物流体系。鉴于在智能电网建设中,主、辅供应链存在的潜在风险和管理失控的可能性较大的弊端,在加强供应商管理的同时,还应从竞争机制上,改善与重构现有供应链结构,以提高供应链的合作水平。具体做法是在供应商之间建立的合作伙伴关系上,能够实现更高层次的整合,通过确立战略合作伙伴,以共同的战略目标与战略计划,同步进行智能电网建设与管理,参与供应商的研发,但这需要供应链上的各节点在组织、文化、管理机制及其人员上,经过长期的沟通、冲突和融合才能实现。

(3) 提高供应链管理的敏捷性。可以从三方面入手：一是加强运作机制。以电网企业为核心,建立统一的供应链管理制度,使整个供应链在资产管理方面具有更高的优越性,实现在物资流、信息流、资金流三条主要工作流的协同管理。二是构架信息平台。构建统一的供应链信息管理平台、通过共享的信息资源数据仓库,实现大量历史数据、业务资料和供应商信息的集成。三是引入现代仓储管理方法,逐步实现准时化采购,有效地控制库存、仓储及物流等费用,对抢修用的备品备件实现虚拟库存管理,保证紧急状况的及时反应。优化仓储网络。

(4) 应用现代物流信息技术。信息技术是建设现代物流体系的基础。地理信息系统,卫星定位系统,射频识别技术等,已经在物流企业开始应用,具有广阔前景。与智能电

网的有机结合必然产生良好的效应。

参 考 文 献

[IAGS2010] Cindy Hurst. China's Rare Earth Elements Industry: What Can the West Learn? Institute for the Analysis of Global Security (IAGS), 2010.

[PWC2011] Raman Chitkara. Continued growth China's impact on the semiconductor industry 2011 update. PWC, 2011.

[FedEx2006] Linda M. Taylor. Speeding the Supply Chain From China How Manufacturers Are Winning with Full Service Shipments. FedEx, 2006.

[J2009] Jeanie M. Larson . The Federal Government Role in Cyber Securecity. Information Systemx Security Association of Orange County, 2009.

[FIAS2007] FIAS. Corporate Social Responsibilicty in China's Information and Communications Technology (ICT) Sector. Business for Social Responsibility, 2007.

[BPG2012] Bryan Krekel. Occupying the Information High Ground: Chinese Capabilicties for Computer Network Operations and Cyber Espionage. Northrop Gruman, 2012.

[H2006] 哈玉涛.供应链信息管理问题研究.2006.

[Y2011] 杨育鹏.论我国海外项目控制采办风险的有效策略.时代经贸,2011.

[Z2010] 左晓栋.美国政府 ICT 供应链安全政策和措施分析.专题研究,2010.

[L2004] 刘泳.提高我国供应链管理水平的思考.2004.

[GJ2006] 国家信息化领导小组. 2006—2020 年国家信息化发展战略.2006.

[Y2011] 闫世刚.我国政府 ICT 采购市场开放性评价研究.科技管理研究,2011.

[QJ2007] 祁莉丽.我国供应链风险管理的现状与对策.安徽农业科学,2007.

[YH2008] 杨辉.我国产业结构优化中的技术标准战略.印刷质量与标准化,2008.

[ZS2012] 张帅.工业控制系统安全现状与风险分析—ICS 工业控制系统安全风险分析之一.计算机安全,2012.

[XPH2004] 薛鹏昊,韩绍清.供应链—现代企业的信息化管理方式.黑龙江科技信息,2004.

[XM2009] 徐曼,沈江.电网企业供应链建模及其应用.工业工程,2009.

[ZN2013] 智能电网中的信息安全技术.北极星智能电网在线. http://chinasmartgrid. com. cn.

[GY2012] 工业控制系统信息安全的探讨与实现—创建“本质安全”的控制网方案应用. http://www. gongkong.

[JXL2002] 蒋秀兰,张晓凤.我国发展供应链管理的思考.承德民族职业技术学院学报,2002.

[LYQ2008] 刘友权.制约我国企业供应链管理发展的因素分析.当代经济(下半月),2008.

[ZT2005] 朱彤.公共标准导航 ICT 走向—ICT 产业公共标准的贸易与技术创新效应. WTO 经济导刊,2005.

[YGW 2005] 杨光伟,曲晓芳.我国物流信息化的现状研究.内蒙古科技与经济,2005.

[ZS12012] 张帅.工业控制系统安全风险分析.信息安全与通信保密,2012.

[MFF2005] 毛丰付,张明之. ICT 产业标准竞争与国家利益.世界经济与政治论坛,2005.

[LM2009] 刘玫.我国供应链管理发展的现状及趋势.科技信息,2009.

[XMH2007] 徐明华,史瑶瑶.技术标准形成的影响因素分析及其对我国 ICT 产业标准战略的启示.科学与科学技术管理,2007.

[BK2007] 本刊编辑部. 呼唤ICT. 信息网络,2007.
[QH2007] 秦海. 如何认识和贯彻国家信息化发展战备. 中国信息界,2007.
[ZG2006] 宗刚,赵红涛. 中国供应链管理发展分析与展望. 金融经济,2006.
[GMZ2003] 高梦昭,张文杰. 供应链企业的信息化问题研究. 物流科技,2003.
[LT2005] 吕铁. 论技术标准化与产业标准战略. 中国工业经济,2005.
[YH2008] 杨辉. 我国产业结构优化中的技术标准战略. 航天标准化,2008.